PRACTICAL ISSUES WHEN DESIGNING AN INFORMATION ACCOUNTABILITY FRAMEWORK FOR eHEALTH SYSTEMS

Nuwan Randike Gajanayake
BSc. (Hons.)

Submitted in fulfilment of the requirements for the degree of
Doctor of Philosophy

School of Electrical Engineering and Computer Science
Science and Engineering Faculty
Queensland University of Technology

May 2013

To My Parents and Chandhi

Keywords

Access control, digital rights management, eHealth, electronic health records, information accountability, information privacy, legal issues, technology acceptance

Abstract

There is rising interest in information privacy management through information accountability (IA) in the computer science discipline. Although accountability is a well established concept in many other disciplines, it is fairly new to computer science. The principles of IA are, therefore, unclear. However, the underlying concept of IA shows potential for information privacy management in the electronic world.

eHealth is one of the most complex man-made informatics ecosystems in the world. Information security and privacy issues have hindered its' proliferation since its emergence. Conventional information security and privacy management measures are deemed unsuitable for a specialised and information intensive domain such as healthcare and therefore, eHealth. In this thesis, we introduce IA to eHealth as a means of information privacy management. To that end we present an Information Accountability Framework (IAF) and introduce Accountable-eHealth (AeH) systems, which deal with information privacy issues arising from internal user activities (i.e. information access and use by healthcare professionals - HCP). Three main aspects related to information accountability are addressed in this thesis, namely: social aspects, technical aspects and legal aspects, which create the Information Accountability Framework (IAF).

We delve into the problem by defining a set of principles of IA and contextualising them to eHealth based on a series of domain specific stakeholder requirements, which reveal that information privacy management in eHealth involves balancing competing concerns arising from the different stakeholders' eHealth requirements; namely, patients and HCPs. To address the technical aspects, first, we introduce a novel access control model that can reach a balance between eHealth stakeholder requirements. Second, we present an architecture for AeH systems with IA capabilities. We use the Open Digital Rights Language (ODRL) as the rights expression language for AeH systems to show how privacy and usage policies can be managed in AeH systems.

To address the social and legal aspects of AeH systems, questionnaire surveys and a case study are presented. The first stage of the survey focuses on the attitudes of future healthcare professionals towards the designed AeH system. An empirical research model is designed and validated that can predict the acceptance of AeH systems. The second stage focuses on the consumers' perspective on AeH systems. A second empirical research model is designed and validated. The case study focuses on the Australian eHealth system and shows how AeH systems can be implemented in the existing eHealth system and legal framework in Australia.

This thesis contributes to the existing body of knowledge in several principal aspects. First, it identifies a set of principles of IA and contextualises them in eHealth. Second, it presents and validates two empirical research models that can predict users' intention to adopt AeH systems. Third, it presents and validates a novel access control model that captures stakeholder requirements towards building AeH systems. Fourth, it presents and validates a technical architecture for AeH systems together with an approach of policy representation and management in the architecture using a DRM technology. Fifth, it presents a case study that shows how the designed IAF is feasible within the current eHealth system and legal framework in Australia.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ACC	–	Acceptance
AeH	–	Accountable-eHealth
ANX	–	Computer Anxiety
ATT	–	Computer Attitude
BI	–	Behavioural Intention
CSE	–	Computer Self-Efficacy
DAC	–	Discretionary Access Control
DRM	–	Digital Rights Management
EE	–	Effort Expectancy
EHR	–	Electronic Health Records
EMR	–	Electronic Medical Records
GP	–	General Practitioner
HCP	–	Healthcare Professional
HA	–	Healthcare Authority
HIPAA	–	Health Insurance Portability and Accountability Act
HL7	–	Health Level Seven
IA	–	Information Accountability
IAF	–	Information Accountability Framework
IC	–	Information Control
ICT	–	Information and Communications Technology
IG	–	Information Governance
IPP	–	Information Privacy Principles
MAC	–	Mandatory Access Control
MySQL	–	My Structured Query Language
NEHTA	–	National E-Health Transition Authority
NPP	–	National Privacy Principles
ODRL	–	Open Digital Rights Language
PBAC	–	Purpose Based Access Control
PC	–	Privacy Concerns
PCEHR	–	Personally Controlled Electronic Health Record
PE	–	Performance Expectancy
PHP	–	PHP: Hypertext Preprocessor
RBAC	–	Role Based Access Control
REL	–	Rights Expression Language
TPT	–	Third Party Trusts
WHO	–	World Health Organisation
XACML	–	eXtensible Access Control Markup Language
XML	–	eXtensible Markup Language

Statement of Original Authorship

The work contained in this thesis has not been previously submitted to meet requirements for an award at this or any other higher education institution. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made.

Signature: _____

28/05/2013

Date: _____

Acknowledgements

I would like to begin by thanking my principal supervisor Dr. Tony Sahama and my associate supervisor Prof. Renato Iannella for their guidance, invaluable expertise, patience and support rendered during the three years of my PhD. Your guidance was invaluable, thank you. Special thanks go to QUT and NICTA for funding my PhD project, without which, this would not have been possible.

I would like to thank my dear wife, Chandhi, for offering her unconditional love and support throughout my PhD, especially during hard times. I would like to thank my parents for bringing me up and teaching me valuable life lessons, which undoubtedly guided me through this unique journey. My thanks extend to my brother and my sister and also to Chandhi's family, who is now part of mine.

My dear friends at QUT, my time here would have been very different without you around me. Your support and encouragement was a blessing.

I would also like to thank the anonymous reviewers of my research papers for giving me valuable feedback. Your suggestions were enlightening. Finally, I extend my thanks to all those who weren't mentioned here for your support.

Publications Arising from this Thesis

The outcomes of this thesis have been published or under review in peer-reviewed journals and conferences.

Published Papers

Refereed Journal Papers

1. Gajanayake, Randike; Iannella, Renato & Sahama, Tony R. (2011) *Sharing with care: an information accountability perspective*. IEEE Internet Computing, 15(4), pp. 31-38

Refereed Conference Papers

2. Gajanayake, Randike; Iannella, Renato; Lane, Bill, & Sahama, Tony R. (2012) *Accountable-eHealth systems: The next step forward for privacy*. In 1st Australian eHealth Informatics and Security Conference, 3 -5 December 2012, Perth, Western Australia. **Best Paper Award**
3. Gajanayake, Randike; Lane, Bill; Iannella, Renato, & Sahama, Tony R. (2012) *Legal issues related to accountable-eHealth systems in Australia*. In 1st Australian eHealth Informatics and Security Conference, 3 -5 December 2012, Perth, Western Australia.
4. Gajanayake, Randike; Iannella, Renato, & Sahama, Tony R. (2012) *Information accountability with policy languages for e-Health*. In AIS International Conference on Information Resource Management (Conf-IRM), AIS, 21 - 23 May 2012, Vienna University of Economics and Business, Vienna.
5. Gajanayake, Randike; Iannella, Renato, & Sahama, Tony R. (2012) *Privacy oriented access control for electronic health records*. In International World Wide Web (WWW) Conference Workshop on Data Usage Management on the Web (DUMW), ACM, 16 - 20 April 2012, Lyon Convention Centre, Lyon, France.
6. Gajanayake, Randike; Iannella, Renato, & Sahama, Tony R. (2012) *An information accountability framework for shared eHealth policies*. In International World Wide Web (WWW) Conference Workshop on Data Usage Management on the Web (DUMW), ACM, 16 - 20 April 2012, Lyon Convention Centre, Lyon, France.
7. Gajanayake, Randike; Iannella, Renato, & Sahama, Tony R. (2011) *Privacy by information accountability for e-health systems*. In 6th International Conference on Industrial and Information Systems, ICIIS 2011, IEEE, 16-19 Aug 2011, University of Peradeniya, Sri Lanka.
8. Gajanayake, Randike; Iannella, Renato, & Sahama, Tony R. (2011) *Information accountability for online healthcare social networks*. In

International Conference on Innovation and Management, IAM 2011, 12 - 15 July 2011, Kuala Lumpur, Malaysia.

Papers under review

Refereed Journals

9. Gajanayake, Randike; Iannella, Renato; Lane, Bill, & Sahama, Tony R. *Accountable-eHealth systems: The next step forward for privacy*. Electronic Journal of Health Informatics. **Invited Paper**

   (Submitted on 03rd February 2013)

10. Gajanayake, Randike; Sahama, Tony R & Iannella, Renato. *Towards a model of acceptance of Accountable-eHealth systems by future healthcare professionals: An Australian perspective*. BMC Medical Informatics and Decision Making.

    (Submitted on 29th May 2013)

11. Gajanayake, Randike; Iannella, Renato, & Sahama, Tony R. *Access control requirements for accountable-eHealth systems.* Electronic Journal of Health Informatics (eJHI).

    (Submitted on 27th May 2013)

12. Gajanayake, Randike; Iannella, Renato; Sahama, Tony R. *Principles of Information Accountability: An EHealth Perspective*. International Journal of E-Health and Medical Communications.

    (Submitted on 30th May 2013)

Preamble

Chapter 1: Introduction

In this chapter, we contextualise the research project. Section 1.1 presents an outline of the research. Section 1.2 presents the background of the research and section 1.3 identifies a knowledge gap. Section 1.4 presents the research problem and section 1.5 formulates the objectives and the research questions. Section 1.6 identifies the significance and scope of the research. The research methodology is presented in section 1.7 and a conceptual map of the research is presented in section 1.8. Finally, the chapter is concluded with an outline of the remaining chapters of this thesis in section 1.9.

1.1 OVERVIEW

An immense growth in the use of Information and Communications Technology (ICT) in healthcare has been witnessed during recent times. It has produced many different applications for providing better quality healthcare in a more effective and efficient manner. The use of ICT in healthcare has given rise to several disciplines such as medical informatics, health informatics, biomedical informatics and clinical informatics that have a common underlying goal. The primary goal of use of ICT in healthcare is to improve the delivery of healthcare to the patients and maintain the quality by protecting the integrity of the information. The complex nature of the healthcare domain itself is one of the main impediments to the successful use of ICT in healthcare. This makes it a challenging undertaking that needs to be successfully executed in order to provide quality healthcare as of public demands.

Given the recent advancements of ICT and its role in healthcare, the needs of the modern healthcare practitioners as well as the public (patients) are different from what we have seen and experienced in the recent past. Healthcare professionals want easy and timely access to reliable information to assist in the decision making process to help improve the quality of care. Patients want control of their health information and demand better management of their sensitive healthcare information for better information privacy and assurance. The healthcare industry generates a huge volume of data from hospitals, primary care surgeries, clinics, laboratories etc.

It is still a challenge to manage such information in spite of decades of experience in the successful application of ICT in other information-intensive industries. Despite the complexity of use of ICT in healthcare, countries such as Australia (among others) have embraced the new technologies and are working towards bringing their benefits to the consumers. On the 1st of July 2012, the Personally Controlled Electronic Health Record (PCEHR) system was made available to the Australian public. The PCEHR system enables every Australian to create and manage an individual electronic health record (EHR). The primary goal of the PCEHR is health information sharing. It gives patients the control over their healthcare records and allows them to manage documents within their EHR. The PCEHR was launched after two years of extensive research and development by the National E-Health Transition Authority (NEHTA). Although there have been meticulous efforts by both NEHTA and government departments in the development of the PCEHR, it is said to reach its full potential in 10 years. This highlights the gravity and complexity of using ICT in healthcare delivery processes.

With the practical benefits of using ICT in healthcare come many inherent drawbacks. Information interoperability, information security and information privacy concerns are high on the agenda. Current developments in this domain have recruited the Internet as the main communication media. These developments are called *eHealth* applications. Manipulating sensitive patient information using the Internet means that the vulnerability of information being disclosed to unintentional entities is far greater. This aspect, among others, augments the aforementioned information security and information privacy issues. Information privacy concerns of patients in eHealth applications are a significant factor that contribute to the impediments for eHealth systems and has to be addressed appropriately.

The application context which this research focuses on is eHealth. eHealth is becoming a more familiar term in the society as ICT support in healthcare practices increases and becomes available for different applications in daily life. When the term becomes broader, underlying concerns such as information privacy and other related issues like trust and adoption also expand and become more significant. Recently, we have seen many attempts made to address these issues to make eHealth systems more robust and to increase the trust towards high consumer adoption. These efforts are focussed mainly on security related technologies such as rigid access

control for healthcare information systems, in other words, preventive technologies. But for a complex, specialised and knowledge driven domain such as healthcare, purely preventive approaches are inapt.

As regards to the above concerns, we introduce information accountability (IA), a concept that is based on *appropriate-use* of information followed by *after-the-fact* accountability for intentional misuse of information, to eHealth. We show that IA can be used to address the information privacy conundrum and can successfully balance eHealth requirements. We present an Information Accountability Framework (IAF) and introduce *Accountable-eHealth* (AeH) systems, eHealth systems that utilise IA. Throughout this thesis we assume that an operational electronic health record (EHR) system exists in a secure and trusted environment that links to the eHealth application we are focused on.

1.2 BACKGROUND

Healthcare is the *world's largest most complex manmade ecosystem* (Mills, 2007). It is a fundamental human need and right. As stated above, the impact of ICT in the progression of healthcare is immense mainly with the increasing demand for efficient and cost effective healthcare delivery (Grimson, Grimson, & Hasselbring, 2000). The users of eHealth technologies can be categorised into three; the *healthcare authority* (HA), the *healthcare professionals* (HCP) and the beneficiaries or *consumers* (patients). A healthcare authority can be the department of health and ageing, state and territory health authority (e.g. Queensland Health), health statutory boards, hospital executives/management. Healthcare professionals include doctors, nurses, pharmacists, diagnostic clinicians, allied health and clinical support staff who provide services to patients in care delivery settings and consumers are individuals who receive care from the health services of the country, including citizens, permanent residents, work permit holders and others. The successful use of ICT in healthcare that is fair to all categories is a challenging undertaking that needs to be successful in order to provide quality healthcare.

Healthcare is a domain driven by information and specialised expertise. A purely preventive approach for data protection governed by the consumers, similar to most available approaches (e.g. access control in eHealth), is not suitable to healthcare because not all consumers have the relevant knowledge to make a

decision as to what information is required to make a decision in a given episode of care. The consumers, therefore, need be encouraged not to withhold any medical information from their caregivers which could be valuable for making a potentially lifesaving decision. But the nature of the information and the ramifications of inappropriate use of that information such as embarrassment, insurability, harm to social status, employability etc. could prevent consumers from disclosing valuable information about their medical history to their caregivers. As stated by Goldman et al. (2000),

> "[without] trusting that their most sensitive health information will be safeguarded, patients are reticent to fully and honestly disclose their personal information and may avoid seeking care altogether" (Goldman & Hudson, 2000).

The Australian Department of Health and Ageing state that;

> "Privacy is a fundamental principle underpinning quality health care. Without an assurance that personal health information will remain private, people may not seek the health care they need which may in turn increase the risks to their own health and the health of others. Indeed consumers regard health information as different to other types of information and consider it to be deeply personal" (Australian Government Department of Health and Ageing, 2004).

This calls for a sense of trust need to be conferred to consumers to encourage them to fully and honestly disclose their medical history to healthcare providers via eHealth systems.

All relevant/required information must be available to the HCPs who make critical decisions about a person's health. In the mean time, consumers has to be assured that the information they have disclosed would not be misused resulting in information privacy breaches. The use of information therefore needs to be controlled. However, if tight access restrictions and rigid security barriers are enforced on healthcare information, the decision making time and effort of HCPs will increase and critical time will be lost that could have made the difference between life and death of a patient. So, *How can healthcare information be made readily available to those who require it and yet be kept safe from being unnecessarily exposed?*

1.2.1 The eHealth Ecosystem

eHealth promise benefits to patient care through enhanced access to information and efficiencies in healthcare delivery (Scott, 2010). The World Health Organisation (WHO) defines eHealth as *'the combined use of electronic communication and information technology in the health sector'* (World Health Organisation, 2012). Considering the current developments, this broad definition can be narrowed down to state that eHealth uses the Internet as the medium of communication allowing for an assortment of capabilities to be introduced to the healthcare domain. Many definitions to the term eHealth have been put forward by researchers in the domain.

According to Eysenbach (2001), eHealth is;

> "[the] intersection of medical informatics, public health and business, referring to health services and information delivered or enhanced through the Internet and related technologies. In a broader sense, the term characterizes not only a technological development, but also a state-of-mind, a way of thinking, an attitude, and a commitment for networked, global thinking, to improve health care locally, regionally, and worldwide by using information and communication technology" (Eysenbach, 2001).

This definition of eHealth highlights that eHealth encompasses a range of different aspects that cannot be addressed through a set of common policies and guidelines suitable for all. Each separate eHealth initiative must consider the characteristics of its target community (state, territory or country) such as its own unique expectations, healthcare system, economic status, legal framework and even the nature of its population and geographical characteristics. Similar definitions have been put forth by others (Deluca & Enmark, 2000). eHealth is a combination of technologies such as the Internet, computer telephony/interactive voice response, wireless communications. Contextually, these technologies can be referred to as eHealth technologies, the Internet being the most prominent.

The proper implementation of eHealth systems will be the solution to many problems associated with today's healthcare. As Kwankam (Kwankam, 2004) agrees by saying,

> "E-Health systems are essential to keeping pace with the exponential growth of health information and to applying this knowledge to resolving world health problems".

These efforts have resulted in the introduction of new legislation such as HIPAA (Mercuri, 2004), and healthcare standards such as HL7 (Beeler, 1998; Schloeffel, Beale, Hayworth, Heard, & Leslie, 2006), openEHR (Beale, Heard, & Kalra, 2007), ISO 27799 health information (Fraser, 2006), CEN 13606 health information (Schloeffel, et al., 2006) and several other standards introduced by OASIS. These standards aim to achieve a consistent baseline for reusability, interoperability and scalability.

Impact of eHealth

The Internet has become a source of healthcare information for many patients as a means of gaining knowledge of their medical conditions. According to Harrison and Lee (2006), 86% of people who have access to the Internet have used it to search health related information. 50% of consumers have demonstrated interests in accessing their information through the Internet. 33% consider switching providers to communicate electronically to their physicians. Ball and Lillis (2001) claim that today the Internet facilitates crucial components of healthcare delivery, including consumer education, disease management, clinical decision support, physician/consumer communication and administrative efficiencies. The word 'patient' is slowly transformed into 'consumer' because of the Internet and the demand for a more active role in their own care. According to Deloitte and Touche, as stated by Ball and Lillis (2001), "[patients] do not receive literature about their medications. They, therefore, take the education to their own hands". In 1999, 74% of US Internet users searched for online medical information. This has resulted in a change in the physician/patient relationship (Xie, Dilts, & Shor, 2006).

The nature of the Internet and that of the healthcare domain raises a number of concerns in regards to the security and integrity of the information. Health information is considered one of the most sensitive in any informatics domain (Cavoukian, 2006) thus, ensuring the security of the information is paramount for eHealth systems to be successful in delivering the capabilities it promises. But the medical environment has a poor history of uptake and implementation of security

measures, as security has traditionally been seen as a business concept (P. A. Williams, 2007).

Electronic Health Records

The main information repository for eHealth systems are electronic health records (EHR) and electronic medical records (EMR). In the heart of eHealth we find EHRs and EMRs. Ferriera et al. (2003) agrees to this notion by referring to EHRs (referred to as electronic patient records or EPRs) as the "Holy Grail" of electronic healthcare information systems. Miller and Sims (Miller & Sim, 2004) say; "of all the health information technology in current use, the electronic medical record (EMR) has the most wide-ranging capabilities and thus the greatest potential for improving quality"; thereby agreeing that EMRs are one of the most important components of electronic healthcare.

Even though EHRs and EMRs are used synonymously in literature, there is a subtle difference between these two terms. Garets and Davis (2005), as cited by Kahn and Sheshadri (2008), defines EMR and EHR as follows;

An EHR is,

> "[an] application environment composed of the clinical data repository, clinical decision support, controlled medical vocabulary, order entry, computerized provider order entry, pharmacy, and clinical documentation applications. This environment supports the patient's EMR across inpatient and outpatient environments, and is used by healthcare practitioners to document, monitor, and manage health care delivery within a healthcare delivery organisation" (Kahn & Sheshadri, 2008).

An EHR is,

> "[a] subset of each care delivery organisation's EMR, and is owned by the patient; it has patient input and access that spans episodes of care across multiple healthcare delivery organisations within a community, region, or state (or in some cases, the entire country)" (Kahn & Sheshadri, 2008).

Essentially, EMRs are medical records of a consumer created and maintained locally by an HCP (or healthcare organisation) and an EHR is a comprehensive medical records shared by all HCPs. Hence a consumer may have more than one EMR but only one EHR. EHRs are a powerful tool for HCPs given their

completeness and availability. EHRs are more beneficial than EMRs mainly because care givers are capable of accessing a patient's entire medical history rather than parts of it as with EMRs. An EHR system can be made available to care givers from anywhere with a suitable Internet facility. For example, HCPs can access it from their local practice, use all capabilities provided for them by the EHR system without having to invest in an expensive EMR system which can be a significant and costly investment for many practices (Yaffee, 2011). EHR systems however, bring with them their own risks.

1.2.2 Information Privacy in eHealth

As stated above, information privacy is a key issue which arises in eHealth and is a key governing principle of the patient-physician relationship (Appari & Johnson, 2010). Information privacy itself can be viewed through two distinct lenses: patient privacy and provider privacy. Although provider privacy is an issue that has to be addressed, the more significant barrier for eHealth adoption is consumers concerns of information privacy (Anderson, 2006). A patient's health record contains sensitive information such as medical diagnosis, medical images, treatments, psychological profiles, employment history, and physician's subjective assessments of personality and mental state (Appari & Johnson, 2010; Mercuri, 2004) and the inappropriate disclosure of these types of information could render the patients to issues such as embarrassment, insurability, child custody cases, and even employment (Cannoy & Salam, 2010; W. Pratt, K. Unruh, A. Civan, & M.M. Skeels, 2006a). When using sensitive information about patients through the Internet and other communication media (eHealth activities), the danger of the security of information being compromised is increased. Given the complex flow of health information in modern healthcare systems (see Figure 2.6), these concerns are further augmented.

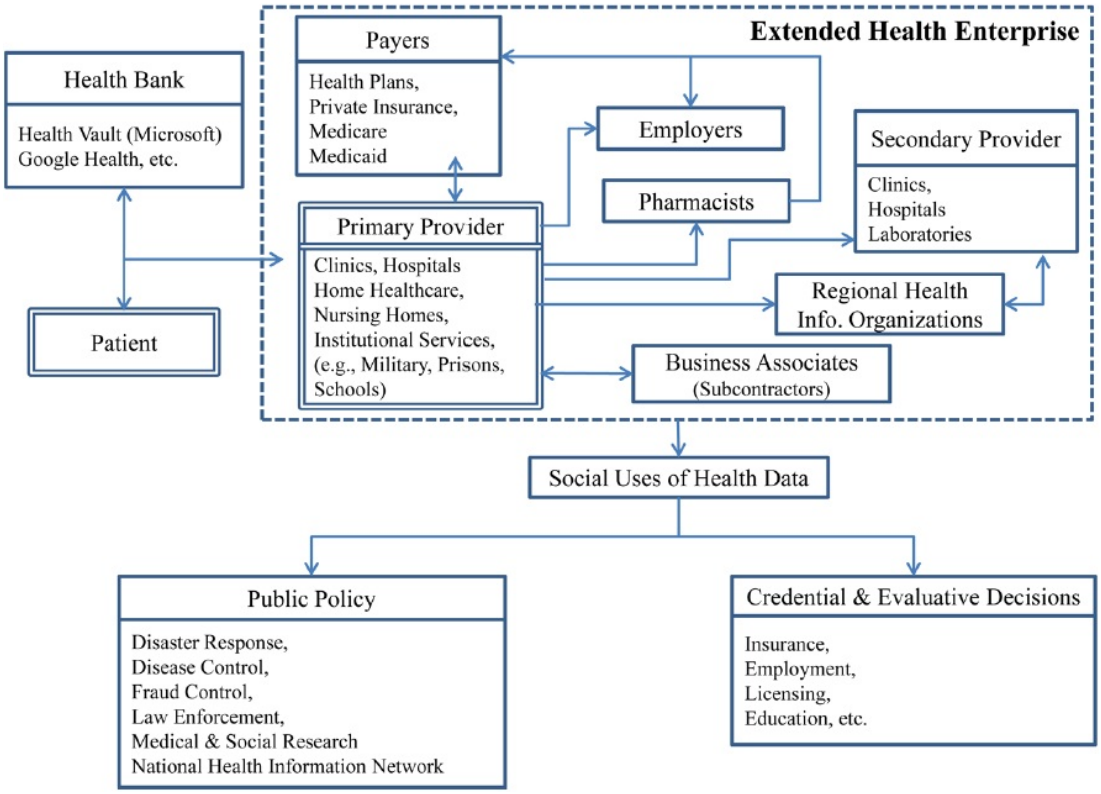


Figure 1.1 Information flow in a healthcare system (Appari & Johnson, 2010)

The complexity of the modern information manipulation processes has given rise to new threats to healthcare information (Mercuri, 2004). In light of these threats, the patients demand better protection of their sensitive information. And the success of eHealth systems depends on how well these issues are tackled and delivered to the consumers. The National E-Health Transaction Authority (NEHTA) believes that the success of eHealth systems is clearly based on the privacy awareness of the Australian community (National E-Health Transition Authority, 2011b). Legislation such as the Health Insurance Portability and Accountability Act (HIPAA) (Annas, 2003) of 1996 in the USA are results of attempts to address information privacy in the eHealth domain.

It is clear that the most significant impediment for the proliferation of eHealth systems is patient privacy concerns (Chen, Chang, & Wang, 2010). Therefore, increasing consumer trust in the eHealth systems by addressing information privacy is critical for their success. In order to achieve this, clear attributes for role-based access, policy development, rules on patient privacy at home, data mining rules and technological measures will be needed to ensure the security and privacy of medical data (Meingast, Roosta, & Sastry, 2006).

1.2.3 An information privacy conundrum

Defining information privacy is difficult (Culnan & Williams, 2009; Smith, 1993; Tsai, Egelman, Cranor, & Acquisti, 2011). The most widely accepted definition of privacy by Alan Westin states that,

> "[it is] the claim of individuals, groups, or institutes to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967).

This definition implies a sense of control of information by the owners or subjects. Privacy concerns are usually coupled with information security which mainly involves unauthorised access by external entities. But addressing data breaches by authorised users pose the biggest challenge and it is a significant aspect for eHealth systems. Some even claim that privacy threats are internal factors and not external (Kierkegaard, 2011). Therefore, patients have an expectation of confidentiality in their dealings with any qualified clinician or HCP (Croll, 2011).

In health informatics, the definition of privacy encompasses confidentiality, integrity, availability and accountability (Ishikawa, 2000). The protection of patient privacy has been governed by the Hippocratic Oath (Lasagna, 2001), which says "*I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know*", where the patient-physician relationship remained a cooperative one. But, with the advancement of technology there is a shift in this relationship towards a more regulation and policy driven one (Parks, Chu, & Xu, 2011).

1.2.4 Information privacy threats

Issues and threats to information privacy in eHealth come from several different directions. Data collection, data use and disclosure, unauthorised access, secondary use, errors, balance between privacy policies, clinical users and patient expectation, awareness of privacy practices, EHR design and lack of standards (Parks, et al., 2011).

The collection of healthcare information must be for defined purposes and its use must be for those intended purpose (Croll, 2011; Culnan & Williams, 2009). Healthcare professionals may at times have to disclose patient health information to other healthcare professionals to make informed decisions for better healthcare

delivery (Ishikawa, 2000). But such disclosure may lead to negative ramifications for patients (Neubauer & Heurix, 2011; Sadan, 2001). Unauthorised access to information itself has two categories; internal breaches and external breaches. External breaches occur when outside entities gain access to the system via hacking or other measure. These threats are addressed to a satisfactory level where such incidents are very rare. As regards to internal breaches, the sensitivity of the information has made it necessary for the *need-to-know* principle to be applied when access to healthcare information is concerned (Blobel, Nordberg, Davis, & Pharow, 2006; Ishikawa, 2000; van der Linden, Kalra, Hasman, & Talmon, 2009). It is a measure used to prevent unauthorised access to information by authorised users (internal users). Internal users may abuse their rights due to curiosity reasons or for other ulterior motives (Culnan & Williams, 2009). Thus, access to information by internal users is controlled by preventive measures such as access control, e.g. Role Based Access Control (RBAC), which enforce rigid barriers. But these are not unsuitable for a specialise domain such as healthcare. There is evidence to suggest that the lack of adequate patient information has given rise to serious medical errors (P. Williams, 2011) which threaten patient health. The availability of timely, unrestricted and relevant patient health information to the appropriate HCPs is thus vital.

1.2.5 Privacy preserving technologies (approaches) in eHealth

According to Kind & Silber (Kind & Silber, 2004), because of the open architecture of the Internet, organisational policies and procedures are needed to guarantee the privacy of and integrity of eHealth systems. These policies need to focus on data security as well as other ethical issues pertaining eHealth. Privacy preservation in eHealth is a highly active research area. It encompasses issues such as anonymity, authentication, authorisation, confidentiality, deniability, unlinkability and EHR data structure (Slamanig & Stingl, 2010). Despite a range of different efforts by researchers, information privacy still hinders the proliferation of eHealth systems. Although most privacy related research is based on information governance policies, technical solutions have also been proposed. Most of the technical solutions proposed for this problem are based on rigid access control measures. Comprehensive reviews of the related work are given in chapters five and six.

1.2.6 eHealth Requirements

Following a careful investigation of the healthcare related expectations of eHealth stakeholders, we have identified two types of eHealth requirements. These requirements have to be carefully addressed in order for a successful eHealth system to be implemented.

Requirements of Healthcare Providers

Timely and relevant information to the healthcare providers is a fundamental requirement in the healthcare domain. As regards to healthcare professionals, we can formulate a set of requirements that are deemed necessary for healthcare professionals. The following requirements of healthcare providers (both individual and the healthcare organisation) were identified that need to be addressed in the development of an eHealth system.

1. **A healthcare authority should have the capability to define their security policies within an organisation**: We identified that a governing health body should have the capability to formulate policies with regards to information access (Ray & Wimalasiri, 2006). These policies, however, should be within the available legislation regarding health information manipulation.
2. **Healthcare professionals need easy access to the relevant information in a non restrictive and timely manner**: Rigid restrictions to health information could hinder healthcare delivery (P. Williams, 2011). Therefore a suitable policy should be put in place for information availability for healthcare providers.

3. **Healthcare providers need to have the capability to share patient health information with other health specialists to make well informed decisions**: Information sharing is seen as a valuable capability and powerful tool (Adler-Milstein & Jha, 2012) for health professionals whilst making a decision (Richardson & Asthana, 2006; Whiddett, Hunter, Engelbrecht, & Handy, 2006a). This capability should not be identified as a special circumstance and be addressed separately. Rather it has to be a familiar activity to health professionals within the EHR system such that when in doubt information can be shared amongst other health professionals to make a well informed decision. Therefore, we believe that this activity should be integrated to be easily achieved within the EHR system.

4. **A healthcare authority should have the power to override the patients' security settings in certain circumstances**: Policies set by patients give the caring health professionals a sense of what the patient requires in terms of confidentiality. But the policies set by a patient may not always be beneficial to the patients, e.g. in a life threatening emergency situation. In such or other justifiable circumstances, the caring health professional should have the capability to override policies set by patients towards delivering appropriate care to the patient (Ferreira et al., 2006).

5. **The need to distinguish between data items and access and usage policies assigned to them**: This requirement follows from the need to segment health information contained in EHRs to enable information to be shared amongst healthcare professionals, which would not otherwise be possible due to privacy requirements of the patients. This requirement also addressed issues related to data collection and the definition of indented purposes. This has also been identified by the standards and Interoperability framework in their data segmentation for privacy pilot study (The Standards and Interoperability Framework, 2012).

In some circumstances it has been identified that the health professionals need to hide certain information from the patients. For example in mental health related situations (Alhaqbani & Fidge, 2008). This is a very sensitive subject within the healthcare domain itself. We consider these as special circumstances. The specific health information in question can be removed or hidden from the patients from the

point where the EHR is created at the health authority's end. But the caring health professional (a mental health specialist) will have the access to relevant information with the consent of a party nominated by the patient as for example the *next-of-kin* at the point of EHR creation. Therefore, we do not consider this as general requirement for healthcare professionals.

Requirements of Consumers

A patient's healthcare information may contain sensitive information such as sexual health, mental health, addictions to drug or alcohol, abortions, etc. This makes such a patient demand strong security for their eHRs. These requirements cannot conflict those discussed above to prevent legitimate healthcare activities from being hindered. We note however, that in the PCEHR (National E-Health Transition Authority, 2011a) system proposed by NEHTA, all privacy settings are set by the patients. Therefore such conflicts will not arise in their proposed system and will hinder healthcare professionals' information needs. The following capabilities were identified as requirements of a patient with an eHR in terms of access control.

6. **Patients need to be able to allow only a preferred (selected) set of healthcare professionals to access their EHR**: A patient needs to have the capability to determine which health professionals have access to their health record (Alhaqbani & Fidge, 2008; Ray & Wimalasiri, 2006). These healthcare professionals are considered as trusted health professionals. But their use of information will still be governed by underlying usage policies set by the governing health authority.

7. **Patients need to be able to hide certain health information from health practitioners who already have access to their EHR**: Patients prefer to hide certain health information such as their sexual health details from certain healthcare professionals who already have access to the EHR (Alhaqbani & Fidge, 2008). However, the information patients hide from a healthcare professional should not hinder their care delivery activities. For example, a patient cannot hide his sexual health details from a dermatologist because there is a strong relationship between those two data types. These relationships can be captured by the policies defined by a healthcare authority.

8. **Patients need to have the capability to see how their EHR is manipulated by users who have access to it**: Although access to the information is managed by access policies, the usage of the information after retrieval is still an open question. Therefore, a patient may be capable of monitoring how the health professionals use the information they retrieve from the EHR.

9. **The administration process of the security settings need to be easy to understand and handle**: Patients cannot always be considered to have a certain degree of technology competency. Therefore, the systems developed should take in to consideration the ability of the general public of managing such a system (Alhaqbani & Fidge, 2008). The management of their EHR therefore need to be an easy task which is familiar to them.

It is important to note that access restrictions might not always be beneficial to the patient. While fulfilling these privacy requirements under no circumstance must the patients' health compromised. In the following chapters, we will refer back to these requirements and show how each of them are satisfied.

1.3 A GAP IN THE KNOWLEDGE

The above requirements reveal that information privacy and the need for healthcare information are competing concerns and need to be addressed appropriately considering domain constraints. To that end, we have identified a series of requirements from both the consumers' and the healthcare providers' perspectives. The current approaches are limited in addressing these requirements towards reaching an appropriate balance of requirements. As a solution we propose the said IAF for eHealth systems. To that end, we observe a gap in the knowledge in terms of information accountability as a measure for privacy management in the eHealth domain. Principally, information accountability has not been defined in eHealth and its underlying principles are unclear. In order for such a concept to be applied to a complex domain such as healthcare, it is imperative that issues such as its technical aspects, stakeholder perspectives and legal aspects are investigated in detail.

1.4 RESEARCH PROBLEM

Challenges in the eHealth domain relate to balancing the requirements of its different stakeholders to achieve the maximum benefits of what eHealth has to offer. Patients expect a certain degree of confidentiality from the health professionals who treat them (Croll, 2011) whilst the healthcare professionals demand easy access to all relevant information related to their patients health. We believe that the concept called *information accountability* (IA) can be utilised in the eHealth domain to achieve this balance. IA means "*the use of information should be transparent so it is possible to determine whether a particular use is appropriate under a given set of rules and that the system enables individuals and institutions to be held accountable for misuse*" (Weitzner et al., 2008).

Figure 1.2 shows a realistic scenario of information flow between different entities and domains. It also shows how information accountability fits in an existing eHealth framework.

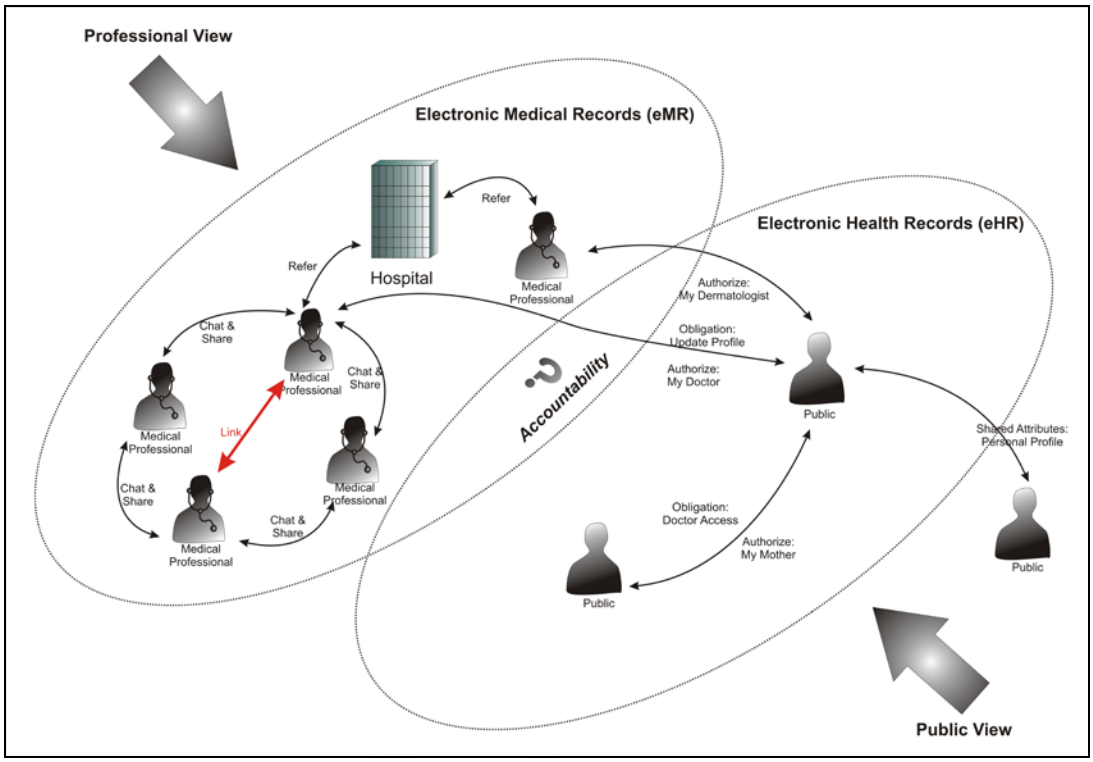


Figure 1.2 eHealth Scenario (Gajanayake, Iannella, & Sahama, 2011).

In the scenario, we can see how a patient's healthcare information might flow in the eHealth domain. We identify that when information flows between the two domains, a mechanism should be in place to control the way in which the data is used

by the professionals and to ensure the public of the security of their sensitive information. This mechanism can be implemented as an information accountability framework (IAF).

In this research, we focus on *appropriate-use* of sensitive health information by healthcare providers in an eHealth system. To our knowledge, there are no available methods or guidelines for applying IA to address the abovementioned issues of eHealth. Therefore, we undertook this research project to lay the foundations towards utilising IA in eHealth. We investigate the concept of IA in the eHealth domain. We investigate how IA, being a fairly new concept to computer science, can be applied to the eHealth domain to overcome its drawbacks in terms of balancing the information privacy needs of patients and the information needs of healthcare professionals. We believe this balance must be achieved in order to have a successfully implemented eHealth system that is adopted by the stakeholders. We also investigate how such systems, if developed, would be accepted by the future consumers of eHealth.

1.5 OBJECTIVES

This thesis aims to identify the applicability of information accountability when addressing eHealth requirements related to consumer information privacy and the design of an information accountability framework (IAF) for eHealth. The specific objectives of this study can be identified in terms of the research questions in section 1.5.1.

1.5.1 Main Research Question

The key question answered in this research is:

"*Can information accountability address the issues related to information requirements and information privacy requirements in the eHealth context?*"

The research question above can be subdivided into specific objectives that answer the thesis of this research. They are as follows:

1. Identify the requirements of eHealth stakeholders that need to be addressed relating to healthcare information.
    a. Identify the information requirements of healthcare providers.
    b. Identify the information privacy requirements of patients.

2. Identify the principles of information accountability.
    a. Identify the principles of information accountability in computer science.
    b. Identify the principles of information accountability in the eHealth context.
3. Identify the technology solutions that address the requirements identified in question 1 in terms of information accountability?
    a. Identify the access control requirements of eHealth in terms of information accountability.
    b. Design a technical architecture for an IAF in eHealth.
    c. Identify the technology requirements to meet the capabilities of the IAF in an eHealth environment.
4. Identify the impact of information accountability on stakeholder acceptance of the IAF in terms of empirical research models.
    a. Identify the aspects related to the acceptance of information accountability by future healthcare professionals.
    b. Identify the aspects related to the acceptance of information accountability by eHealth consumers.
5. Identify the implementation aspects of the IAF within an existing eHealth environment; namely, in the Australian context.
    a. Identify the current approach to eHealth in Australia.
    b. Identify how the designed IAF fits within the current Australia eHealth landscape.
    c. Identify the legal issues related to the IAF in Australia.

By achieving these research objectives, we make a valuable contribution to the existing body of knowledge as to how eHealth systems can be implemented with the use of IA principles to overcome the barriers discussed. The research questions are addressed by each chapter as follows.

Section 1.2 addressed research objective 1 by identifying a series of requirements of eHealth stakeholders. Chapter two addresses research objective 2 and formulate foundations for the subsequent chapters. Chapters three and four fulfil

research objective 4 though quantitative and qualitative survey results. In chapter five a novel access control model is presented that captures the essential elements for the design of a technical architecture for the IAF and fulfils research objective 3(a). Research objectives 3(b) and 3(c) are addressed in chapter six with the design and validation of the said architecture. Chapter seven presents a case study of the applicability of the IAF in an existing eHealth infrastructure focusing on the Australian eHealth system, which fulfils research objective 5.

1.6 SIGNIFICANCE AND SCOPE

As we have seen, conventional restrictive approaches to managing information are not suitable for an information intensive domain such as healthcare. We have identified that information privacy of eHealth consumers is a significant factor in their proliferation in the healthcare domain. Although important, we do not consider the privacy requirements of healthcare professionals, which are not currently seen as significant contributing barriers for eHealth adoption. Thus, information privacy concerns of eHealth consumers are addressed through information accountability in this thesis.

Information accountability has not yet found its way into common practice, especially in eHealth. Through this research study it is intended that there will be a significant contribution to knowledge in the eHealth domain in terms of information accountability and a better understanding of the concept in eHealth. It is also the expectation that this work will assist in future research that will also contribute to the knowledge which will ultimately be adopted in the healthcare sector for better delivery of healthcare services for the general public.

In an exploratory study of this nature it is important to perceive the limitations. Given the time constraints and the requirement of the knowledge and expertise of several other domains including medicine, we do not aim at implementing a working prototype of the IAF. Proposed semantic reasoning capabilities are not implemented in this thesis. Although technical protocols that have been designed are formally defined and expressed using formal specification languages, a mathematical formalism will not be considered given the exploratory nature of the study. Such formalisms, which require the consideration of implementation constraints, may be

done in future work. This thesis will serve as a starting point for work in information accountability in eHealth applications, which is absent in the eHealth domain.

1.7 METHODOLOGY

The approach of the research project is illustrated in this section. The research project was divided into four phases. Figure 1.3 depicts the different phases of the research project. Phase 1 involved a comprehensive literature review and problem definition. Two surveys were conducted, including a pilot survey, to measure the attitudes towards information accountability in the eHealth domain in phase 2. Phase 3 involved the technical aspects of the research project. The results from the survey were taken into consideration for the development of a novel access control model for AeH systems, which was validated via a Web based prototype. A technical architecture was designed and validated via the same prototype and a model checking approach. The final phase of the research was the investigation of different aspects of the IAF to demonstrate its functionality and suitability in the Australian eHealth system via a case study. The results from the four phases validate the designed IAF.

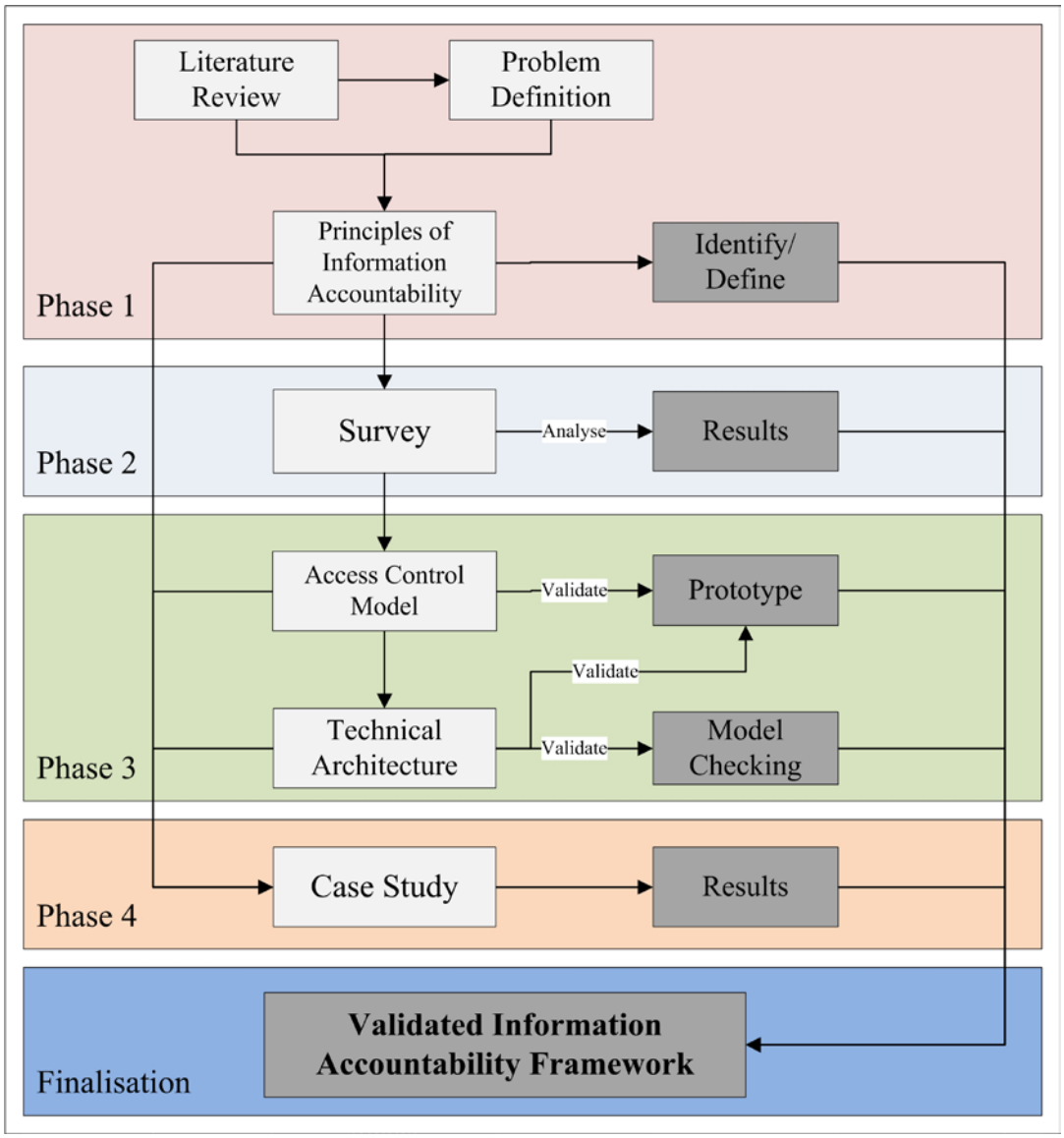


Figure 1.3 Research outline

1.8 RESEARCH MAP

The chapters of this thesis are interrelated to form a logical structure beginning from theoretical foundations of IA and then investigating them in the social domain proceeded by the presentation of technical aspects of IA in eHealth and finally with the presentation of a case study, which primarily discuss the legal aspects related to the IAF in the Australian eHealth system. Figure 1.4 shows a map of the research with all the components. The IAF in question consists of three main aspects: social, technical and legal. The IAF is presented in the form of these components by providing supporting evidence for each component.

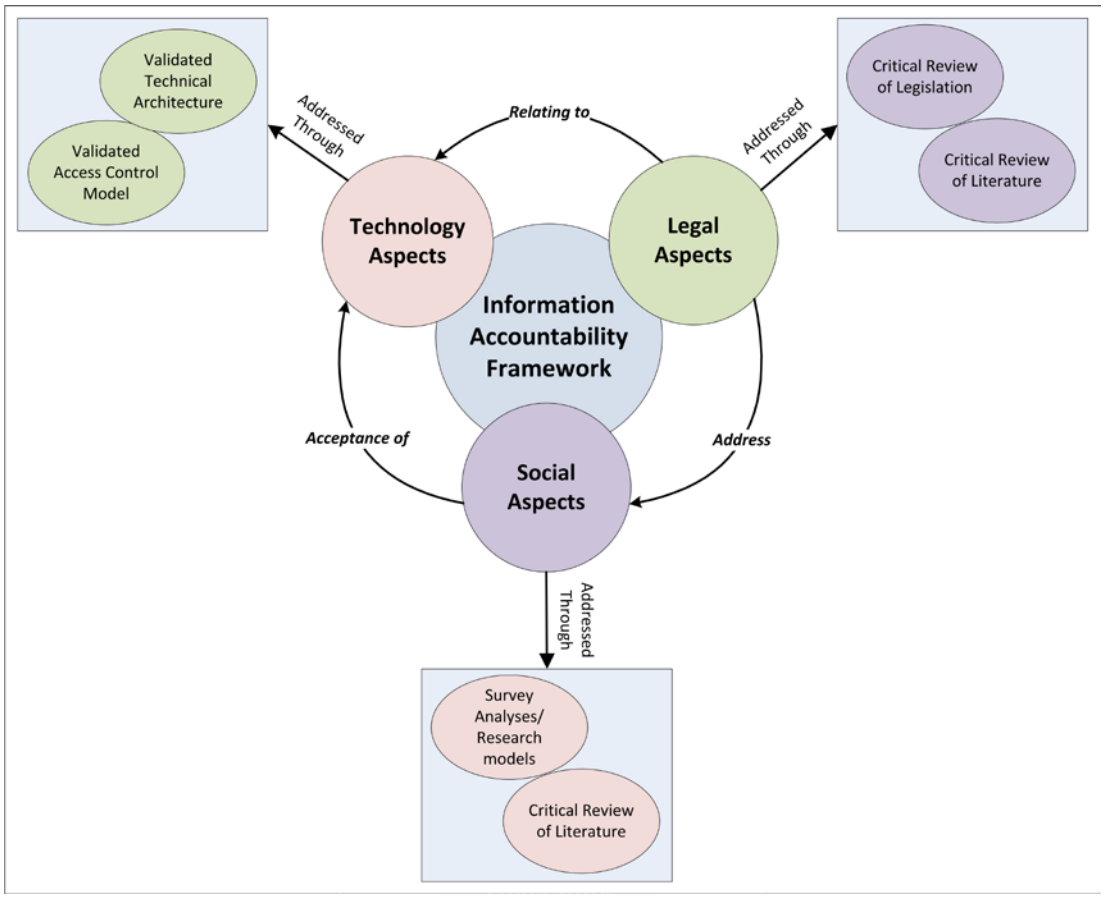


Figure 1.4 Research map

The social aspects of the IAF are addressed in the first part of the thesis in chapters three and four. Part two of the thesis consists of an access control model and a technical architecture for AeH system presented in chapters five and six respectively. Part three presents the implementation aspects of AeH systems, focusing mainly on the legal aspects as depicted in Figure 1.4, in the form of a case study of the Australian eHealth system in chapter seven.

1.9 THESIS OUTLINE

The rest of this thesis is arranged as follows.

Foundation

- Chapter 2: Principles of Information Accountability

Part One: Social Aspects

- Chapter 3: Views on Information Accountability in eHealth: A Survey of Future Healthcare Professionals

- Chapter 4: Views on Information Accountability in eHealth: A Consumers Perspective

Part Two: Technical Aspects

- Chapter 5: Access Control Requirements for Accountable-eHealth Systems
- Chapter 6: A Technical Architecture for Accountable-eHealth Systems

Part Three: Implementation Aspects

- Chapter 7: The IAF in the Australian eHealth System: A Case Study

Closure

- Chapter 8: Conclusions and Future Work

Foundation

Chapter 2: Principles of Information Accountability in eHealth

In this chapter, we present the principles of information accountability. The chapter follows work done on information accountability in computer science in general and establishes a series of principles that must be present in accountability systems. These principles are then contextualised in eHealth to emphasise how they must be used to address the contextual requirements towards successful implementation of eHealth systems augmented with information accountability. We introduce Accountable-eHealth (AeH) systems; eHealth systems augmented with information accountability principles and discuss their characteristics to conclude the chapter.

2.1 INTRODUCTION

Information accountability (IA) is a solution for usage control on the decentralised Web (Feigenbaum, Hendler, Jaggard, Weitzner, & Wright, 2011; Weitzner et al., 2008). Appropriate policy representation, policy aware transaction logs and policy reasoning are key components of IA on the Web (Weitzner, et al., 2008). IA is about holding the information users answerable for their actions and the ramifications of those actions. Weitzner et al. (2008) propose a transparent audit process which gives the users incentives to abide by the policies put in place and the ability to determine whether a particular use of information is policy compliant. Though the concept is nothing new, IA is a comparatively new concept to computer science and ICT and has been interpreted in various dimensions by computer scientists. These approaches have been carefully systematised by Feigenbaum et al. (2012) and have made a valuable contribution by stating that the term "accountability" is far broader than just anonymity, identification or exposure and that it allows actions to be tied to consequences and violations to be tied to punishment. The approaches considered by Feigenbaum et al. (2012), however, define IA in a general point of view. Being a concept of various dimensions, IA has to be defined contextually for its applicability to be better understood. The lack of contextual definitions of its underlying principles makes it difficult to apply in complex domains. Information systems which utilise the principles of IA are called

accountability systems. Current technological advancements, especially in the semantic web domain, eliminate the technical barriers previously present in implementing this type of systems. The success of any accountability system depends on the policy formulation, which in turn depends on the context in which the systems are designed.

IA can address many different issues in a vast array of disciplines. Usage control is one area of interest to computer scientists through which the privacy conundrum can be addressed. Privacy has been and still is a major obstacle when it comes to information systems' adoption and trust. When dealing with information privacy, we have to consider several factors: the type of policies, the type of participants and their requirements, data ownership, data provenance, and the nature of the information (such as sensitivity and availability). These aspects differ significantly with the context. As already discussed in chapter one, in terms of information management through electronic media such as the Internet, privacy can be defined as the degree of control given to the subject of the information (Westin, 1967) although have argued that confidentiality addressed privacy. But confidentiality is a matter of giving the owner, not the subject, the control of the information. It is important, therefore, that the roles of users are clearly defined within the context when looking to address information privacy. Here again, we point out that data ownership depends on the context we consider. Within a given context, the policies differ in terms of user requirements and other external factors such as government regulations and organisational policies. Data provenance is another important aspect when it comes to dealing with violations of policies or misuse of data. It can also play a critical role when the trustworthiness (Alhaqbani & Fidge, 2009) of the data and users become factors. The nature of the information is the main reason why privacy becomes a critical factor for information systems in the first place, as is the case in the healthcare domain. It is crucial that the nature of the information is properly evaluated and the proper policies are put in place to govern its use.

Therefore, as a means of addressing the issues identified in section 1.2, we introduce information accountability to the eHealth domain. To this end, we formulate a series of principles drawn from prior research and the general requirements for information accountability to be implemented in computer science.

We contextualise them to eHealth and lay foundations for the remainder of the thesis. We begin with a critical review of the related work.

2.2 RELATED WORK

What is accountability? According to Boyd (Boyd, 2003), responsibility and accountability are used interchangeably by many people. They are like the two sides of the same coin. Responsibility, Boyd says, involves what we are required to do, i.e. our duties. Accountability is when someone holds us answerable for our actions and their outcomes. In other words, responsibility reflects only up to the point of decision and accountability focuses on the ramifications after the decision is made (Boyd, 2003; Eriksen, 2002). Emanuel et al. (Emanuel & Emanuel, 1996) have this to say about what accountability is. "Accountability entails the procedures and processes by which one party justifies and takes responsibility for its activities". The essence of all this, when focusing on information accountability, is that the user of the information is held liable to explain, justify or answer for their use of information, when requested by the party to whom the information belongs. The significance of information accountability in information intensive domains is highlighted from the statement below.

> "Information is widely available and the use of that information needs to be controlled. Rather than enforcing rigid up-front control over the use of information, there is a need to accommodate fair use. The control over the use of information is imperfect and exceptions are possible, but violators can be identified and held accountable" (Weitzner, et al., 2008).

When investigating information accountability, transparency is one of the most important aspects that also need to be taken into account. Transparency and accountability will be critical in helping the society to manage the privacy risks that accumulate from the explosive progress in communication, storage and search technology (Weitzner et al., 2006). The subjects of information must have the privilege to observe how their information is used and by whom. Transparency can be defined differently in two contexts. In business ethics and information ethics, it's likely that transparency refers to the visibility of information. In computer science and ICT, it is more likely to refer to the invisibility of information (Turilli & Floridi, 2009). Despite the contradicting definitions in different contexts, by transparency what we mean here is that information held about a consumer is visible to that

consumer (giving consumers the right to see the data held about them) and so is the use (access to) of that information by anyone else so that any action could be traced back to an individual. As Weitzner et al. (2008) state, "transparency and accountability makes bad acts visible to all concerned", hence referring to the visibility of information usage, clarifying our distinction.

According to Ferreira et al. (2003) the lack of success in large information-dependent areas such as hospitals is due to its deficient usability and poor security. Unlike paper-based systems, that have evolved through many years, where accountability processes are well understood, digital systems have very different and complex processes. The need for transparency and accountability is ever more important in information systems which are becoming ever more complex and decentralised (Weitzner, et al., 2006).

> "Transparency in data manipulation and inference enables users to have a clear view into the logical and factual bases for the inferences presented by the system. Accountability in data manipulation and inference enables users or third parties to assess whether or not the inferences presented comply with the rules and policies applicable to the legal, regulatory or other context in which the inference is relied upon" (Weitzner, et al., 2006).

Another aspect that comes to light related to accountability is provenance. When holding someone accountable for access and use of a particular set of information, the reliability of the information as well as the information known about the transactions are also important to guarantee the correctness of the accountability process. Provenance deals with the history of information so that the source of the information can be traced back when needed to guarantee that the information is authentic. Cheney et al. (Cheney, Chong, Foster, Seltzer, & Vansummeren, 2009) say that provenance is not easy to define. Many have defined this according to their different needs and applications. In general, provenance can be defined as information about the origin, context or history of the data. They believe that provenance will help develop many factors of quality information use including transparency and accountability.

What is provenance in electronic data? Moreau et al. (2008) point out that electronic data does not have the necessary historical information that would help end-users, reviewers or regulators make the necessary verifications. In computer

systems, a data's provenance is represented by process documentation, says Kifor et al. (2006). Guaranteeing the provenance of information on accountability is without doubt one of the most important questions that need to be addressed when developing an accountability framework.

2.2.1 Theoretical background of information accountability in computer science

Information accountability is a relatively new concept to computer science and ICT. Though limited, there is much effort in the current state of research to formalise information accountability in computer science. We will present an account of these efforts here.

Information accountability is the subject of many researchers. They have either defined or implicitly used the term accountability in various dimensions. A serious concern for accountability systems is the lack of formal foundations. Formalising information accountability has been widely explored by several prominent researchers, especially in the information privacy domain (Feigenbaum, Hendler, et al., 2011; Feigenbaum, Jaggard, & Wright, 2011; Jagadeesan, Jeffrey, Pitcher, & Riely, 2009; Sloan & Warner, 2010; Weitzner, et al., 2008). It is the claim that a purely preventive approach to security and privacy is inadequate (Feigenbaum, Hendler, et al., 2011; Kagal & Abelson, 2010) that has driven work on information accountability in recent times. Feigenbaum et al. (Feigenbaum, et al., 2012) investigate some existing frameworks for accountability and explore whether deterrence is a better term than accountability and puts forth a formal model for accountability in terms of punishment (Feigenbaum, Jaggard, et al., 2011). Jagadeesan et al. (2009) make an effort to develop formal foundations for information accountability in terms of the privacy policies which define appropriate sharing of information among agents and provides algorithms that can be used by an auditor to check for compliance with rules. In their approach they focus on after-the-fact verification with recorded audit logs capable of detecting 'untrusted' access of information and assign blame when the privacy contract is violated. They rely on a principle underlying accountability concept that the fear of being caught will deter users from misusing information. A solution to the question of compliance of privacy policies was proposed by Weitzner et al. (2008) by tracking all transactions and making them transparent. They assume that appropriate policy rules exist with a formal representation, policy-aware transaction logs and a policy-reasoning

capability which would enable accountability systems to hold information users (individuals and organisations) accountable for their actions.

Sloan et al. (2010) address information accountability in a broader scope than what has been done by Weitzner et al. (2008) by considering both social policies and technical aspects. They point out that automated checking for compliance of privacy policy is a necessity for accountability systems and without the adequate foundations in both formal models and public policy issues they are unlikely to do so. Many of these approaches to accountability assume that the appropriate policies exist and the requirements and contextual dimensions are captured by them. Sloan et al. (2010) believe that policies required to developing accountability systems are informational norms and state that a proper balance between privacy requirements and competing concerns is necessary to sustain the architectural and social aspects introduced by Weitzner et al. (2008). It should be highlighted that the above mentioned policies and the informational norms are all dependent on context.

Trust is another aspect related to accountability in terms of human interactions (Friedman & Grudin, 1998; Friedman et al., 1999). Due to the interactions people have through electronic media, trust and accountability play a significant role in how people perceive different aspects of their interactions.

Systems that utilise information accountability thus must incorporate many aspects that are not present in current applications. These systems therefore inherit specific characteristics and goals towards information security, information privacy, trust and adoption. The next section discusses accountability systems in detail.

2.3 ACCOUNTABILITY SYSTEMS

A common measure for managing access to information by authorised users is access control. In computer science, access control and accountability are closely related. Access control is about imposing restrictions on users. In other words access control is about prevention. Users are required to prove their authenticity before access to information is granted. These approaches have proven to be successful in the past and in current information systems but brings with them inherent drawbacks. One such drawback is the hindrance to legitimate users to access information. If not that, it is an accepted fact that a purely preventive approach to information security and information privacy is inadequate (Feigenbaum, et al., 2012; Kagal & Abelson,

2010). Information accountability on the other hand is about deterrence. But the *after-the-fact* aspect of accountability may raise concerns over information abuse. This means that a violation must occur for it to be acted upon. This of cause is an inherent characteristic of accountability systems and is addressed through its underlying principles. It is argued that with accountability mechanisms in place, the *online* world would be more like the *offline* world where potential violators are deterred by the prospect of negative consequences (Feigenbaum, 2010). To this end we identify certain goals for accountability systems and are shown in Figure 2.1.

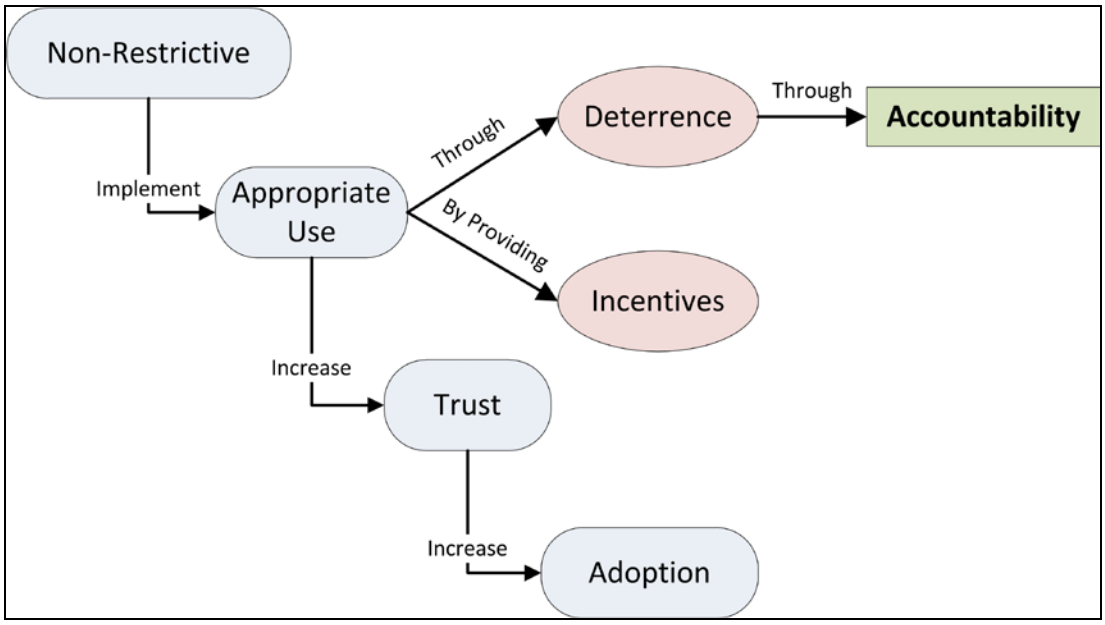


Figure 2.1 Goals of accountability systems

Accountability systems aim at reaching specific goals in terms of how information is manipulated. The main goal is to be **non-restrictive**. They aim to provide information to legitimate users without rigid access restrictions. To this end, they implement **appropriate use** of information. Accountability systems achieve appropriate use by **deterring** users from intentionally misusing information. A fear of being caught is delivered with the presence of **accountability mechanisms** which is appropriately conveyed to the users. **Incentives** are given to the users to follow the procedures and enforce appropriate use. Accountability systems aim at increasing consumer trust in the system. Without consumer trust, it is difficult to implement non-restrictive access/use of information. With the implementation of appropriate use as shown in Figure 2.1, accountability systems hope to gain **trust** of the consumers. With increased trust, systems are **better adopted**.

Creating proper incentives that would make consumers follow rules of accountability systems is an important aspect of accountability systems (Sloan & Warner, 2010). For an information user, the fear of getting caught for intentional misuse of information is an incentive to follow system rules. A strong assurance of security should be given to consumers as an incentive to prevent them from withholding information or enforcing rigid restrictions on data which would be their obvious cause of action to secure their information from being unnecessarily or wrongfully being disclosed.

2.4 PRINCIPLES OF INFORMATION ACCOUNTABILITY

In this section we will formulate and discuss principles of IA which aid in fulfilling the goals of accountability systems mentioned above. A map of the IA principles and some related attributes are shown in Figure 2.2.

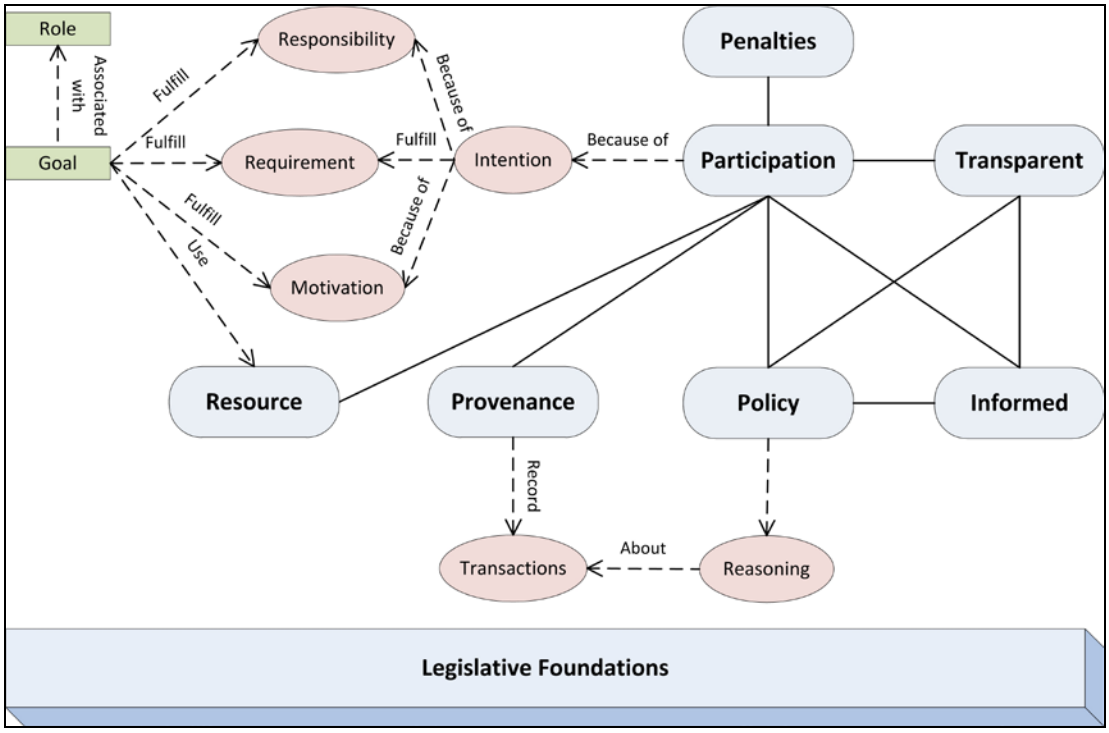


Figure 2.2 Principles of information accountability

In computer science, information accountability is built up on several key principles. Accountability systems must adhere to these principles in order to achieve the expected accountability capabilities and to reach their goals to be non-restrictive and fair use systems. **Participation** of users in an accountability system is a fundamental principle of IA. Users participate in information systems activities to fulfil a purpose. A user's purpose or **intention** to participate in system activities can

be either to fulfil a ***requirement***, because of ***responsibility*** or because of other ***motivations*** for example gathering demographic data for research purposes, which is although not directly related to the normal system operations but is a considerable interaction with the data. Capturing the actual intention of an information user is of great importance to accountability systems and helps in defining usage policies for data objects and users within the system. The role a user plays within an organisation requires him to fulfil certain tasks by manipulating information. Hence a user is said to have certain ***goals*** of strategic interest (Bresciani, Perini, Giorgini, Giunchiglia, & Mylopoulos, 2004). The users perform various tasks to fulfil these goals. It is the aim of accountability systems to manage the way these various tasks users perform within the system to promote fair use of information. Therefore, accountability systems must have the capability to monitor user interactions with the system. IA principles discussed here facilitate this capability. Capturing user intentions and defining the extent to which a user can participate in the information manipulation process is heavily contextual.

The definition of a **resource** is a fundamental principle of IA and so is in any informatics discipline. In the digital arena, resources are digital assets or information artefacts. The account number of a person's bank account is a digital asset. Each asset is different from each other in terms of quality, quantity, sensitivity etc. E.g. Given a person's bank account, he may have only one account number associated with it, but may have more than one credit/debit card with their own unique card numbers associated with that same account. Hence, the data should consist of certain inherent characteristics from the time of creation. The clear representation of the characteristics of digital resources is fundamental but is worth mentioning. This clear definition is vital for accountability systems because the nature of the resource brings with it usage constraints for users. We can couple three types of actors to information resources, the subject of the resource, the owner of the resource and the consumer of the resource. Each of these actors will have inherently different roles to play within the system.

Transparency is a principle of IA that is of utmost importance. All *relevant* users must have the capability to observe how information is used and by whom. Transparency can be defined differently in two contexts. In business ethics and information ethics, it's likely that transparency refers to the *visibility* of information.

In computer science and IT, it is more likely to refer to the *invisibility* of information (Turilli & Floridi, 2009). But Weitzner et al. (2008) states that, "*transparency and accountability makes bad acts visible to all concerned*", hence referring to the visibility of information usage. Therefore, despite the context which we are focused on, by transparency we mean that information transactions are visible to the required entities. This allows for the actions performed by data consumers to be traced back to an individual or process. According to Weitzner et al. (Weitzner, et al., 2006), transparency and accountability will be critical in helping the society to manage the privacy risks that accrue from the explosive progress in communication, storage and search technology. The need for transparency and accountability is ever more important in information systems which are becoming ever more complex and decentralised.

Provenance of electronic data deals with the history or a record of transactions performed on a data object. A record of such would enable computer systems to reason over the life cycle of a data object. As Moreau et al. (2008) point out, electronic data does not have the necessary historical information that would help end-users, reviewers or regulators to make the necessary verifications. The availability of computer based provenance aware systems enable the users to decide whether they trust the electronic data in a computer based information system. Provenance can provide facts about the authenticity of a data object but it plays an even bigger role in accountability systems. When holding someone accountable, the trustworthiness of the data about the inappropriate transaction(s) or the evidence is crucial. Hence, provenance of data and metadata is a significant factor in IA. In IA, provenance is facilitated using appropriate ***transaction logs*** which are an essential component in current information systems (Lampson, 2009). These transaction logs are meant to be policy aware so that the system itself is capable of identifying inappropriate use of data or a breach of policy. Provenance data can be stored in transaction logs in a format that can facilitate ***policy reasoning*** within the system to give the users the capability to reason about misuse and against claims of misuse. The reasoning process includes inquiries about potential misuse of data by the subjects or owners of the data and justifications about the usage by data consumers.

Data consumers have a right to be **informed** of the underlying policies and the ramifications of breach of policies especially when the system facilitates a tracking

process which monitors the transactions by every user. Therefore users of an accountability system should be well informed, i.e. a notification process where users are informed about underlying policies before an action occurs must be put in place. For example, a user will be notified whether he is authorised to access/use a particular set of data he is trying to access and the ramifications if he proceeds regardless of the warning. This will also help in facilitating non-repudiation which is a significant aspect in information security.

In the case where an inappropriate use of information has occurred, the ramification of that occurrence towards the information user needs to be well defined in terms of appropriate **penalties or negative consequences**. In accountability systems (inappropriate) participation is entailed by negative consequences. A sense of awareness has to be delivered to the data consumers in a form they understand in terms of financial, professional, social or legal penalty. This awareness of the consequences is meant to deter users from inappropriate use of information in accountability systems. It will also give the victim or the claimant a sense of one's rights in terms of the use of their information by a third party. It will also aid in increasing consumer trust in the system. These penalties evidently require a legal framework where they can be properly defined.

It is important to understand that the principles presented above must all be governed within a **legislative framework** which defines each aspect clearly. The legal foundations are a critical aspect of accountability systems. For example, if clear definitions of the penalties for violations are not given, the threat of negative consequences that deters users from misusing information will not be conveyed thus failing to provide the necessary incentives to abide by the rules. The legal aspects of IA and accountability systems in the healthcare context are discussed in detail in chapter nine. Next we will discuss IA principles in the healthcare context.

2.5 INFORMATION ACCOUNTABILITY IN HEALTHCARE

Accountability, in general, is a significant issue in healthcare. This entails ethical and professional conduct, professional negligence and other such related issues. Accountability relating to healthcare information manipulation arises mainly as a result of information privacy concerns. According to Emanuel et al. (1996) it is important to clearly identify the different parties in healthcare that can be held

accountable, the issues for which a party can be held accountable and the appropriate mechanisms for accountability in healthcare in order to understand the concept of information accountability in healthcare. The components of accountability, Emanuel et al. (1996) say, are who, what and how. "*Who*" relate to the different parties that can be held accountable and the parties that can hold other accountable. '*How'* are the mechanisms for holding someone accountable. 'What' as they define it are the domains in which someone is held accountable in. Another important component that had to be but was not considered in their approach is the reason or the significance of why hold someone accountable for their actions, or the '*Why*' in accountability. Emanuel et al. (1996) delineate three models of accountability; professional accountability, economic accountability, and political accountability. They continue to say that one model of accountability is simply not enough for a complicated system as healthcare. And, also, the models of accountability should not be confused with the different facets of the healthcare system.

According to Ferreira et al. (2003) the accountability information should be made usable by many stakeholders, each one having a different purpose and, therefore, different access to the information. The Joint Group of the General Practitioners' Committee and the Royal College of General Practitioners as cited by Ferreira et al. (2003) says, in healthcare, this would allow a patient to review some of the actions associated with their electronic patient record (referring to an EHR). Healthcare professionals and auditors would be able to browse summary events as part of their normal work and to search further in extraordinary cases. They state that the main objective of accountability systems is to provide a means to verify, analyse and investigate users' actions. More importantly though, its presence tends to ensure procedures are correctly followed.

2.5.1 The need for Information Accountability in Healthcare

Accountability can address a wide range of aspects of healthcare such as medical negligence, unethical practice, pharmaceutical abuse, etc. In terms of usage control, information accountability mechanisms in healthcare allow to ensure that patient health information is not misused by care providers or other stakeholders. In other words, information is used for the purpose for which they have been collected and only for the benefit of the patient and other legitimate purposes. If we are to achieve information accountability in healthcare, the aforementioned purposes have

to be comprehensively defined. This is a process that must be carried out with the required (domain) knowledge and expertise to determine the relationships (mapping) between data in EHRs and purposes. A simple representation of this is shown in Figure 2.3. This mapping will identify which data element in an EHR is linked to which defined purpose(s). A healthcare professional that is authorised to access a particular data element can access and use it for only the linked purpose(s). But healthcare professionals are allowed to access data which they are not authorised to access but will have to provide justifications for their actions.

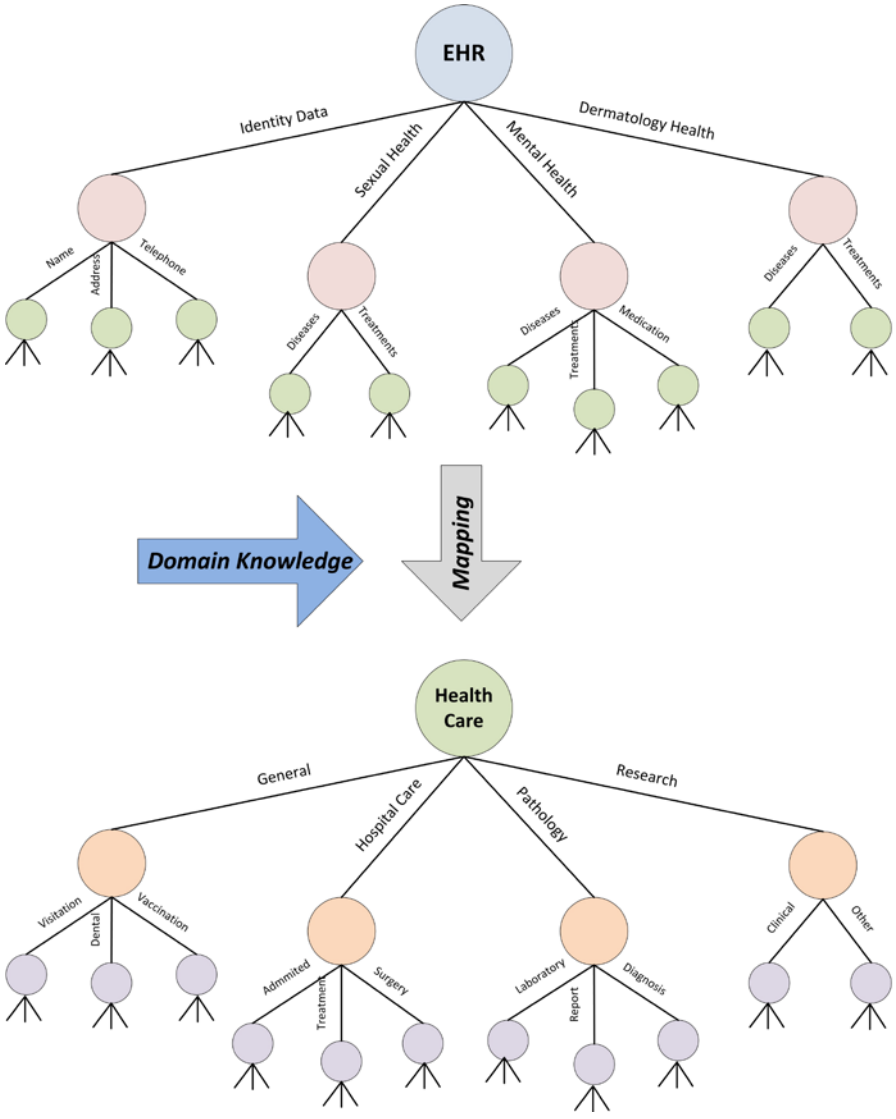


Figure 2.3 EHR data and intended purposes mapping

As brought to notice earlier, data ownership is a critical factor that needs to be properly understood if data usage control is to be achieved. In the healthcare domain

it is difficult to define who owns health information. It is clear that patients are the subjects of health information. But patients are not always medical professionals; hence it is impossible to give them complete control of their health information. Privacy policies of a patient should accompany policies from a professional health body such as a trusted medical practitioner or a central health authority. But it is important to balance between the patient's privacy requirements and the requirements of the healthcare providers or the care givers (competing concerns).

In section 1.2.6, we identified requirements of eHealth stakeholders. We note that the healthcare domain demands that while fulfilling these requirements of stakeholders, under no circumstances must the health of the patient be compromised. Clear procedures for overriding usage policies in emergency situations should be defined to this extent. The nature of the healthcare domain demands the implementation of a *break-the-glass* approach in such situations (National E-Health Transition Authority, 2011a).

Healthcare professionals have a responsibility towards the patients to deliver the best possible care. This responsibility comes with the acquisition of the specialised knowledge which governs healthcare practice. Healthcare professionals seek a degree of confidence in the policies and protocols within an eHealth system and a guarantee of the accuracy of the health information itself. The proper mechanisms should be put in place to deliver this level of confidence of healthcare professionals who are responsible for making decisions towards the wellbeing of their patients.

Defining clear attributes for role-based access, policy development, rules on patient privacy at home, and data mining rules and technological measures will be needed to ensure the security and privacy of medical data (Meingast, et al., 2006). The appropriate management of health information in eHealth systems is therefore a crucial factor. The data contained in eHealth systems can be considered as digital assets. The policies that govern the use of these assets can then be formulated and represented using digital rights management technologies. These policies should cover the requirements of all participants in healthcare and must encompass usage control features in order to gain the trust of patients and the confidence of healthcare professionals.

Controlling how authorised users use information is challenging. As regards this control, we raise the question; "*Will users only use data for the intended purpose(s)?"* In a complex domain such as healthcare which is driven by specialised knowledge, controlling the usage of information by those specialists (HCPs) is somewhat a sensitive matter. It is not always the correct cause of action to impose restrictions to information access and usage on HCPs. But in terms of the privacy requirements of patients some degree of restriction to the usage is necessary to fulfil those requirements. Information accountability with its defined principles can address this issue by reaching a correct balance of the previously identified requirements.

2.6 MOTIVATING CASE SCENARIO

The following case scenario illustrates how different eHealth stakeholders would behave in a care setting. The policy formulation and manipulation processes that are discussed in chapters five and six will follow this case scenario. The case scenario is designed to capture and illustrate how the policy formulation and manipulation protocols fulfil the information privacy and information access requirements identified in section 1.2.6. The activities presented in this scenario can be generalised into any other eHealth scenario that involves similar activities.

Patient X has a comprehensive electronic health record which is managed by a central health authority in his home state called *StateHeath*. StateHealth is responsible for securely storing EHRs of residents of its state and providing certain capabilities to them. StateHealth is also responsible for managing the state's healthcare professionals including physicians, nurses, lab technicians and other relevant staff. StateHealth defines health policies and intended purposes for the data collected and stored in EHRs. These policies fulfil requirements of healthcare professionals and StateHealth itself. Patient X is also capable of setting his own policies on the data elements in his EHR. These policies mostly consist of his privacy requirements. Patient X maintains a list of trusted healthcare professionals who can access all or parts of his EHR depending on the trust level Patient X and StateHealth has assigned for them. All healthcare professionals are required to specify the purpose for which they require access to a set of data before access is granted to them.

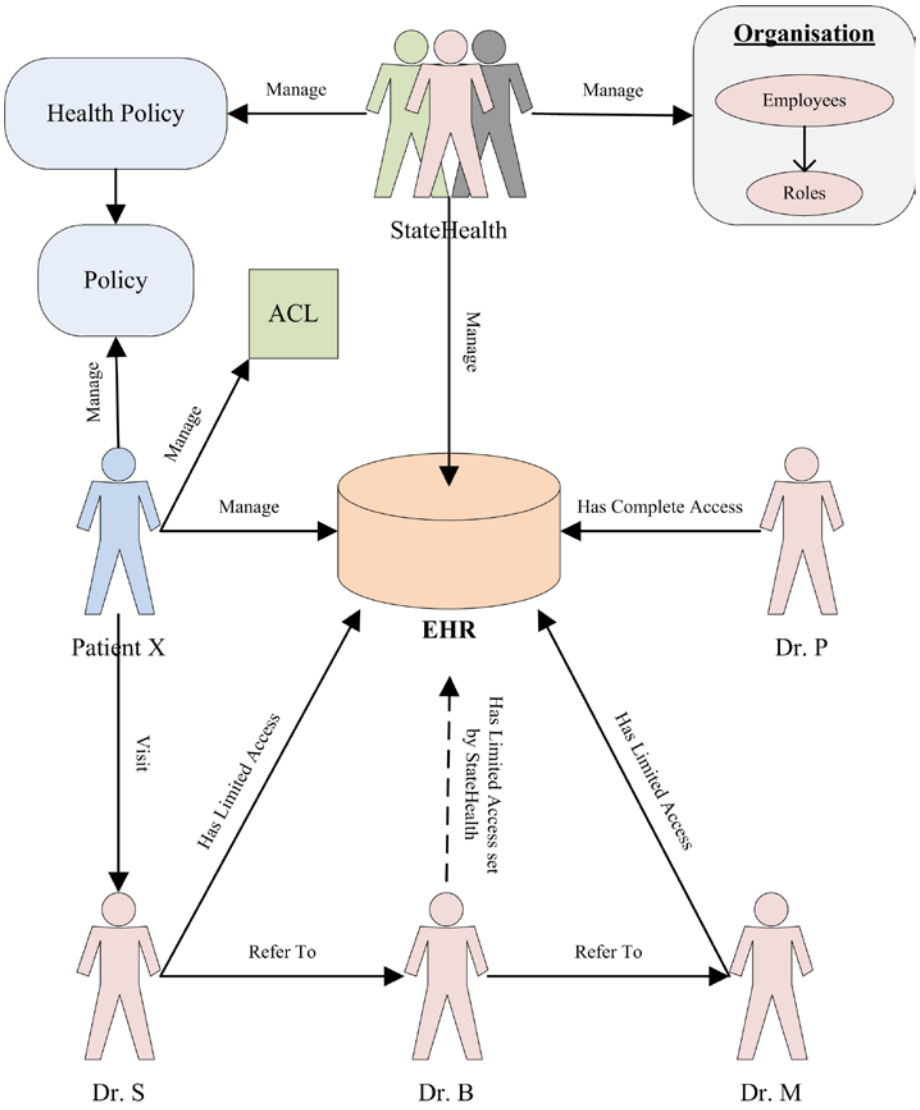


Figure 2.4 Motivating healthcare scenario

After noticing a skin rash, Patient X visits his trusted dermatologist Dr. S for a check up. After the preliminary examination, Dr. S thinks that Patient X's skin condition could be linked to a known sexually transmitted disease (STD). Patient X does not have a sexual health specialist in his list of trusted health professionals. However, Dr. S wants to share Patient X's details with a sexual health specialist, Dr. B, in order to get a specialists' opinion on the situation. Dr. B has a default access level set by StateHealth by being assigned the role of a sexual health specialist. Since Dr. S is in Patient X's list of trusted health professionals, she can initiate a request to share Patient X's (relevant) details with other health professionals. Patient X, however, is notified of this action by Dr. S. After Dr. B gets (and accepts) this request from Dr. S, he initiates a usage request to use the data for diagnostic purposes. Patient X has a history of mental illness and does not want anyone else

other than his GP (Dr. P) and a trusted mental health specialist who has treated him before (Dr. M) to know about it. Dr. B suspects that Patient X's skin condition could be stress related and tries to access his mental health record. At this point, because Dr. B is not authorised to access Patient X's mental health details, he is warned by the EHR system of this fact and Dr. B refers Patient X to Dr. M. Dr. M as Patient X's trusted mental health professional, investigates Patient X's condition and makes a diagnosis. Dr. M may or may not include Dr. B as a specialist in the diagnostic decision making process. After Patient X's illness has been diagnosed and a treatment plan is decided, his EHR is updated by the treating physician(s). Depending on the policy StateHealth has set on EHR updates; Dr. S, Dr. B, Dr. M or Dr. P will make relevant updates to the EHR. After or during this episode of care Patient X may decide to add Dr. B as a trusted healthcare professional in his EHR. We assume that certain medical conditions have relationships between them that give rise to the fact that a particular health professional e.g. a dermatologist who has access to a patient's dermatology details by default (set by StateHealth) should also have default access to the patient's sexual health details. In our scenario above, Dr. S has default access to dermatology details and sexual health details of her patients' and Dr. Bs' access is also set likewise because of the relationship between skin conditions and STDs.

We will use this case scenario primarily to contextualise the principles of information accountability, which is given next, and to demonstrate the protocols presented in chapters five and six. However, the case scenario is referred to in chapters three and four to maintain connectivity of the chapter.

2.7 PRINCIPLES OF INFORMATION ACCOUNTABILITY IN eHEALTH

In this section, we revisit the principles of information accountability discussed above and contextualise them to eHealth. We show how a number of eHealth requirements given in section 1.2.6 are satisfied by the principles of information accountability. The above case scenario is used for this contextualisation.

2.7.1 Participation

In healthcare it is important that responsibility and accountability are carefully balanced (Emanuel & Emanuel, 1996). The reason for this is that healthcare decision making is driven by specialised knowledge and expertise. If accountability measures

are put in place to govern how healthcare professionals, whose knowledge and expertise is invaluable, should ***participate*** in healthcare activities there has to be a fine balance between the responsibility and accountability measures. Therefore, as eHealth requirement 1 states, the healthcare requirement must be expressed in terms of policies set by a governing healthcare authority. Accountability begins where responsibility ends. After making a decision which one is responsible for, the decision maker is accountable for the ramifications of that decision imposed on the subjects or in this case the patients concerned. Each participant in a healthcare scenario can be categorised into roles within the healthcare domain. These roles can be thought to carry out professional tasks to fulfil their responsibilities, requirements and motivations. Hence, the information access requirements must be adequately satisfied, again referring to eHealth requirement 1. We do not however intend to define a comprehensive record of the tasks associated with each role in a healthcare organisation. However we point out that NEHTA (National E-Health Transition Authority, 2011a) has identified several types of roles with different capabilities in their new Personally Controlled Electronic Health Record (PCEHR) system as individuals, nominated representatives, authorised representatives, providers and nominated providers. Policies should be developed that address the different capabilities of roles within the industry. In our healthcare scenario, Patient X has three main rights; the right to decide whether or not to undergo medical treatment, after receiving a reasonable explanation of what the treatment involves and the risks associated with the treatment, the right to be treated with reasonable care and skill by a healthcare provider and the right to confidentiality of information about medical conditions and treatment[1]. Therefore, Dr. S, Dr. B and Dr. M have a responsibility towards Patient X to make the appropriate communications with him and make decisions regarding his health.

2.7.2 Transparency

As discussed in the previous section, ***transparency*** is a fundamental principle of IA (Weitzner, et al., 2006). In the eHealth scenario, Patient X, as the subject of the information, has the right to view what is contained in the EHR, who has access to it and what they do with the data they retrieve as specified in eHealth requirement 8.

[1] Legal Services Commission of South Australia. (2012). Law Handbook Online. http://www.lawhandbook.sa.gov.au/ Retrieved 23 May, 2012

This gives Patient X the confidence to disclose his sensitive health information to the EHR system. StateHealth is responsible for providing this capability to Patient X and all who are registered with them and own an EHR. This transparency can be facilitated through transaction logs which record all transactions of users of the system. Transparency also covers the capability of the patients to make enquiries about suspicious activity by information users, in this case about any potentially suspicious actions performed by Dr. S, Dr. B, Dr. M, or Dr. P and also by StateHealth itself.

2.7.3 Policies

Patients have a fundamental right to confidentiality of information about medical conditions and treatment (Croll, 2011). This should allow patients to set their privacy **policies** within a healthcare information system that manages his/her medical information, thus satisfying eHealth requirements 6 and 7, which can be specified in their privacy policies. However, in a domain such as healthcare it is not always possible to allow every privacy policy of the patients to be operationalised. As stated earlier, healthcare is a highly specialised area which requires specialised medical knowledge to make an informed decision. Therefore, the policies that govern the control of information within EHRs need to also encompass policies formulated with a healthcare perspective, thus we refer back to eHealth requirement 1. In our case scenario, Patient X sets his privacy settings and relevant access rights for the health professionals in his access control list (ACL). StateHealth will also set access policies for the health professionals depending on the role they play in the organisation. For example, Dr. S will be assigned the role of a dermatologist; Dr. P will be assigned a role of a general practitioner and so on. These two policies will then have to be combined to set the final operational policy for the system. In this process, Patient X will be notified of any changes made and the final state of the policy.

2.7.4 Provenance

Data **provenance** is a subject vital to any informatics domain (Moreau, et al., 2008). Here we will briefly discuss what role provenance plays in an eHealth environment. Provenance is an important aspect of any information system, especially if they are Web based. Unlike traditional information systems with network connections to known locations, Web based systems interact with users

from anywhere in the world. This makes it a factor to be able to trace a particular transaction to its source. The open architecture of the Web raises concerns over the legitimacy of the data being recorded and updated. In an eHealth environment this is a significant issue since the data retrieved from eHealth systems are used for diagnosis purposes to treat patients, and if not accurate could lead to adverse effects. Hence provenance plays a significant role in any health related information system. Groth et al. (2012) point out the significance of provenance and presented requirement for provenance on the Web using three hypothetical scenarios. They identified three major provenance dimensions; content, management and use. They raise the issues of reusability of the content of provenance data. This can be directly related to interoperability issues that are of concern in the health informatics domain. Once provenance data is correctly stored in systems, the management of data becomes an issue. To what extent should provenance data be exposed to system actors? Besides providing evidence about the history (e.g. origin, authenticity, creators etc) of a data element, provenance can also provide insights in to the life cycle of a data element. In accountability systems, this relates to making justifications about information use by a consumer with the use of appropriate transaction logs stored with provenance data. In the scenario we presented, if Dr. B has viewed Patient X's mental health records despite being warned not to do so, a notification would have been sent to Patient X informing him that Dr. B's action could be of intentional misuse of his health information. At this point Patient X is able to lodge an enquiry asking for a justification from Dr. B as to why he accessed his mental health records. Under the conditions that users of the systems fall under, Dr. B would then have to provide a justification as to why he accessed Patient X's mental health details. This relates to the requirement that patients should be capable of seeing how their information is being used, as stated in eHealth requirement 8.

2.7.5 Informed

If accountability measures are in place, a proper notification process should also be in place to keep the users well **informed,** in order to prevent repudiation and unintentional misuse of information by delivering the appropriate incentives (Feigenbaum, Hendler, et al., 2011). The system users are aware of the policies in place within the system, their rights and capabilities and the ramifications of breach of policies. These notifications together with the provenance and transaction logs can

also facilitate non-repudiation within the system. They will also give the patients the confidence they need to disclose their sensitive information. However, because healthcare is highly specialised, patients cannot be given the ability to enquire about every transaction and request a justification for the actions from the healthcare professionals. This may hinder the health professionals' professional activities. The system itself should be able to identify possible misuse of data and the patients are given the chance to request a justification for those actions.

2.7.6 Penalties and Legislative support

Legislative support is imperative for accountability systems (Sloan & Warner, 2010). In healthcare, information and privacy are governed by appropriate legislation. The Australian Law Reform Commission (ALRC) took on the task to review the *Privacy Act 1988* to inquire the extent to which it continued to provide an effective framework for the protection of privacy in Australia. In their report, the ALRC made recommendations towards the legislation focused on healthcare information and privacy in Australia (Australian Law Reform Commission, 2008). In a health information system governed by IA principles, the issues concerning information privacy and security as well as the appropriate methods of accountability in terms of **penalties** should be addressed by appropriate legislative constructs. In Australia, the operation of eHealth is subject to several Commonwealth, State and Territory privacy and information protection legislation (Australian Government Department of Health and Ageing, 2004; Australian Law Reform Commission, 2008; Office of Legislative Drafting and Publishing, 2010) and an individual's ability to control who can access their information in certain circumstances are addressed in these legislation (National E-Health Transition Authority, 2011c). Even though there is much attention to the information security and privacy issues in healthcare in a legal perspective, for accountability systems to successfully reach their goals in the healthcare domain, all aspects of IA principles discussed above must be completely and sufficiently covered by proper legislation, especially the aspects of appropriate penalties.

2.8 ACCOUNTABLE-eHEALTH SYSTEMS

So far in this chapter, we have introduced information accountability and formulated a series of principles in the eHealth domain. Towards a novel model of

eHealth augmented by IA, in this section we introduce Accountable-eHealth (AeH) systems. We defined AeH systems as eHealth systems which adhere to IA principles.

Introduction to AeH systems

The goal of AeH systems is to be non-restrictive in terms of information availability to legitimate users. They provide incentives to the users to implement appropriate use of information. These incentives take the form of accountability entailed by penalties (Feigenbaum, Jaggard, et al., 2011). The underlying principle is that when users are aware that such use of information would lead to a negative outcome, they would be deterred from engaging in such activities. Thus, allowing information to be made available for the legitimate user more openly and effectively. In terms of the information owners' perspective, the knowledge of the existence of accountability mechanisms and the transparency of system activities are incentives towards increasing their trust in the system.

The presence of IA mechanisms deters users from intentionally engaging in inappropriate activities. This is more profound in the *offline* world than in the *online* world (Feigenbaum, Hendler, et al., 2011). This deterrence is governed by social norms that are accepted by the majority of the society. But it is not the case in the *online* world. Such norms are still in their embryonic stages and are not clearly defined nor widely accepted in the society. This creates problems for AeH systems. But it is the intention that ones such systems become available and used by the majority of the community, the practices will become norms themselves.

An overview of the accountable-eHealth model

In our model, we consider three types of users; a central health authority, patients, and HCPs. The health authority is the governing body responsible for managing the EHR system and managing its employees i.e. HCPs. The health authority defines default access levels for each HCP relevant to their role within the healthcare domain. The patients define their own access policies for the HCPs they nominate to give access to their health records according to individual privacy requirements. Using a predefined protocol, the two policies are combined such that the final operational policy assigned for each HCP satisfies both the patient's privacy requirements and the HCP's information requirements. HCPs who have been nominated by a patient to have access to his EHR will lodge usage requests containing the required data types and the intended purpose(s) for access. These

requests are processed using a knowledgebase containing EHR data types and related purposes. All usage of EHR data by HCPs is stored as transaction logs for *after-the-fact* accountability purposes. In an event of a possible misuse of a patient's health information by a HCP, the patient is capable of lodging an inquiry to the relevant HCP asking for a justification for the particular usage. If the HCP fails to do so, he is held accountable for the ramifications of his actions. Figure 2.5 shows a simplified AeH model.

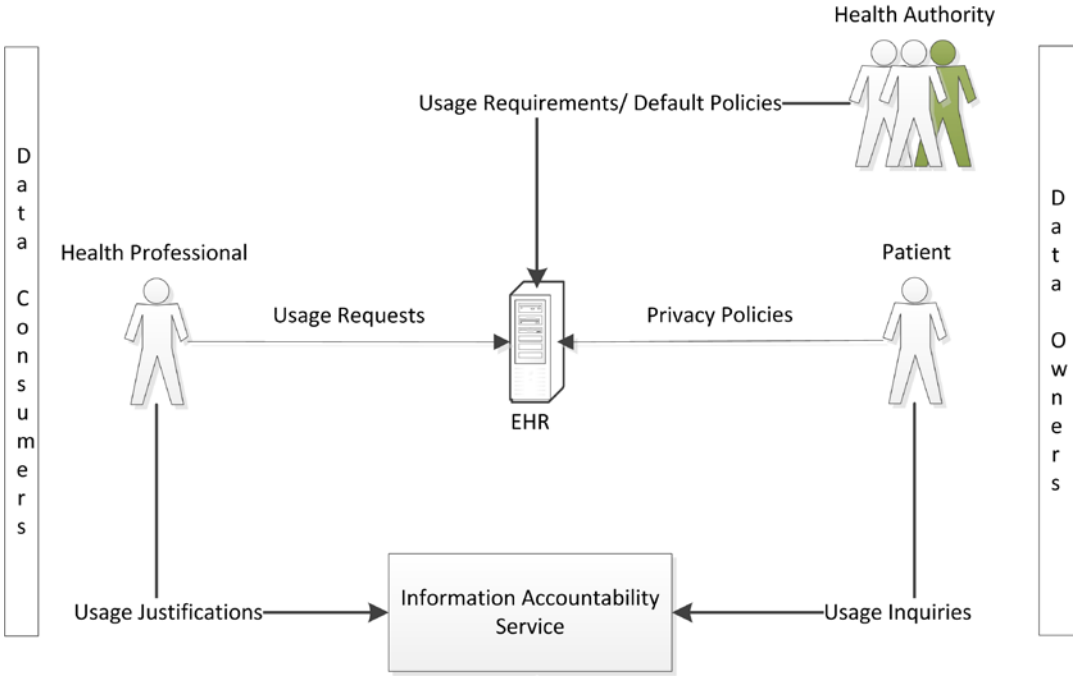


Figure 2.5 Accountable-eHealth Model (Gajanayake, Iannella, Lane, & Sahama, 2012)

A simple use case diagram for the AeH model is shown in Figure 2.6.

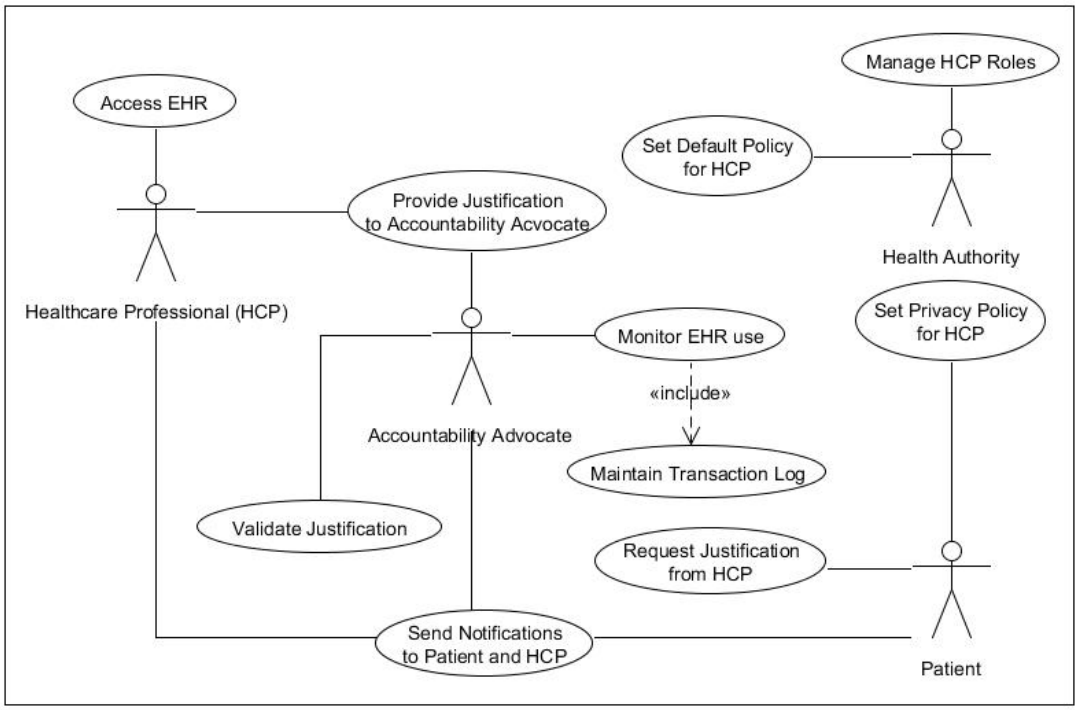


Figure 2.6 Use case diagram for AeH systems (Gajanayake, Iannella, Lane, et al., 2012)

2.8.1 Characteristics of AeH systems

In this section we will discuss the characteristics and protocols of AeH systems arising from the principles IA discussed earlier. The characteristics also follow the eHealth requirements identified in section 1.2.6 in chapter two.

Control of health information

Delegating control of personal information to the subjects has been seen as a means of addressing privacy in information sensitive domains (Haas, Wohlgemuth, Echizen, Sonehara, & Müller, 2011). AeH systems extend control of health information to the patients as well as a governing health authority thus adhering to eHealth requirements 1, 6 and 7. This will ensure that fulfilling patient privacy requirements would not lead to a hindrance to healthcare delivery by HCPs. Policies for how information must be used are set either by the patients, a relevant authority or by both as seen in Figure 2.5. Therefore, in some circumstances a patient's privacy policy may be overridden by that of the health authority, thus adhering to eHealth requirement 4. Patients nominate preferred HCPs to access information in their EHR, adhering more specifically to eHealth requirement 6. The HCPs are assigned specific levels of access as defined in the aforementioned policies.

Information usage and justifications

Health information must be used for the purpose of healthcare delivery for the patients. AeH systems require a comprehensive record of purposes for which information can be used by HCPs. These predefined purposes are maintained by the health authority. Although predefined policies govern the use of information in AeH systems, HCPs are allowed to access information that is outside of those policies to ensure that the required information is available to the HCPs in unforeseeable circumstances. This characteristic of AeH systems thus adheres to what is stated in eHealth requirement 2. This will however trigger an event in the system where the patient in question can request a justification for the use of information from the HCP. The HCP is obligated to justify his actions regarding the patient's health information. A patient may or may not choose to request a justification given the nature of the incident. Providing this capability to the patients enable AeH systems to be more open and patient centric. But it is also important to view this aspect in a HCP's perspective by considering their responsibilities towards providing quality healthcare to their patients. The inquiry and justification process must not hinder the normal healthcare activities of the healthcare professionals. Patients must only be allowed to make inquiries about incidents which cannot be resolved by the information accountability service. The attitudes towards this function will be further investigated in chapters three and four.

Notification

To enforce transparency, AeH systems propose a notification process where all participants are kept informed about the policies and the activities of the system. In this process the HCPs are notified of actions (access to information) that are outside of their allowed capabilities and patients are informed of possible misuse of their health information by HCPs. This would enable patients to be aware of how their health information is being used (see eHealth requirement 8) and HCPs to be more alert towards inadvertently accessing the wrong information.

Provenance

Provenance of electronic data deals with the history or a record of transactions performed on a data object. A record of the activities in the system must be kept in the form of policy-aware transaction logs which act as accountability information

used to validate the above mentioned justifications by HCPs in the event of a conflict.

Penalties and redress

Adequate measures must exist to minimise the extent of negligent or intentional misuse of health information by an HCP. Such measures should ideally be designed to operate both as deterrence against such behaviour as well as incentive for HCPs to act appropriately. These penalties must be communicated to the users such that they are aware of the consequences of intentional misuse of sensitive information.

2.9 DISCUSSION AND CONCLUSION

Information accountability is a fairly new concept to computer science and ICT. The term has been defined in several dimensions by researchers in the computer science arena. We made the argument that information accountability should be defined in a contextual perspective to convey the sagacity of its principles. We have identified and presented the principles of information accountability which accountability systems should adhere in order to reach their intended objectives. We have identified healthcare as a potential domain which can benefit from the principles of IA and the accountability systems goals. Healthcare is a complex information domain due to the nature of the information used and its complexity and specialised knowledge driven nature. The use of specialist knowledge in healthcare is an obstacle to system developers because the requirements of the stakeholders conflict with many aspects of system mostly in terms of policy. The requirements of healthcare consumers have to be fulfilled together with the requirements of the care providers such that conflicts of policies are addressed in such a way that a domain (healthcare) sensitive compromise is achieved. A health record of a patient has to be complete and readily accessible for it to be useful to the care provider.

Information accountability is focused around the way users participate in the system and the policies associated with the data elements they use. It is important for accountability systems to capture the intentions of the users. Users fulfil their intentions by performing certain tasks towards achieving a specific goal. These goals are to be defined within the context the systems operate. In healthcare, a

comprehensive list of intended purposes associated with the data will be defined by an entity with the relevant domain knowledge to do so.

Data in an EHR and the actions users perform on data should have a clear record of provenance in the form of a policy-aware transaction log in order for accountability to be achieved. Provenance of data is a subject of many different aspects. Here we have considered in general the importance of data provenance in healthcare.

Accountability systems have an inherent drawback. This is the fact that actions are taken for misuse of data after the incident has occurred. This *after-the-fact* issue would itself be reason enough for consumers to be concerned of their information in an accountability system. But the concept behind IA is that users will be aware of the consequences of their actions and will deter from misusing data due to the fear of negative consequences, more like in the *offline* society we live in. So it is a matter of facilitating this awareness (informed) and a sense of responsibility (participation) in the consumers through the IA principles.

Accountable systems contain audit logs of every transaction within the system. These logs may become the focus of legal issues which occasionally occur in the healthcare domain. In most of these issues the healthcare professionals are blamed for misconduct or negligence towards the patients. The presence of these types of audit logs may contribute to, for example, the insurability of a health professional who might agree to use such systems. Therefore, health professionals may not accept these accountability mechanisms as a practicable option. This could hinder the accountability systems greatly. This however, can be addressed through proper policies supported by legislation. Proper legislation plays a major role for these types of systems to take effect, particularly the definition of the appropriate methods of accountability in terms of consequences for misuse of data.

In this chapter, we have presented the principles of information accountability in the healthcare context. We have argued that information accountability is a concept better defined in context than in a general sense. With the proper definition of the principles, we identified how eHealth systems should be designed with the use of information accountability to address information privacy and related issues. It is

important to understand that it is next to impossible to fill the *analog* and *digital holes* present in any information system[2]. In our case scenario we are dealing with the visibility of health information to the appropriate user. Once a person obtains the required data, how can we prevent him from showing these data to a bystander on a computer display? How do we track this sort of action? These remain open questions for ethical and professional conduct and cannot be control by policies enforced within computer systems (all trust is within the system).

The development of an accountability system for healthcare involves the collaborative effort of computer scientist, healthcare professionals, legal experts, social scientists and IT professionals. From the available literature, it is clear that information accountability has not been addressed in a healthcare context than in other domains. Together with the developments in ICT and consumer awareness of those technologies and its application in the healthcare domain, information accountability could pave the way forward in terms of information privacy management and usage control of electronic health resources altogether.

[2] Sandhu, R. (2012) *Grand Challenges in Data Usage Control.* Keynote speech at the WWW 2012 Workshop on Data Usage Management on the Web (DUMW), April 16, Lyon, France.

Part One: Social Aspects

Chapter 3: Views on Information Accountability in eHealth: A Survey of Future Healthcare Professionals

In this chapter, we present the results of a survey conducted to measure the attitudes towards information accountability in eHealth. A research model and descriptive analysis of the survey data are presented. The survey data used in this chapter consists of quantitative and qualitative data from 334 completed online questionnaire survey responses from university students studying medicine, nursing and various other health related courses in three leading universities around Queensland, Australia. The findings relate to the attitudes of the participants towards electronic health records and characteristics of AeH systems as presented in chapter two. This exploratory survey was done as an investigation into how the concepts behind an information accountability framework (IAF) would be accepted by potential future healthcare professionals. The results from the survey support, to a certain degree, the applicability of IA principles in the eHealth domain. The findings indicate that there is support from the professionals' perspective for the technological aspects of an IAF presented in chapters five and six. Research objective 4(a) is addressed in this chapter.

3.1 INTRODUCTION

Designing systems that cater for eHealth requirements of different stakeholders is a complex undertaking because balancing these requirements is both a complex and sensitive undertaking. In chapter two, we established a series of principles that govern the use and control of health information which we introduced as principles of information accountability. We saw potential behind those principles for achieving the aforementioned balance of requirements when dealing with EHR systems. There are however no such systems available that can be tested and evaluated. Nevertheless, it is important to measure how these systems, if developed, will be accepted by the eHealth stakeholders.

This chapter draws from the results of chapter two and develop and test a conceptual research model on the acceptance of the IAF in eHealth as well as a descriptive analysis of results of a questionnaire survey as a measure of the attitudes towards the IAF. The research model is primarily based on the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh, Morris, Gordon, & Davis, 2003), a well established and frequently used model of technology acceptance in information systems research. Justification of the hypotheses and the logical reasoning are also drawn from previous technology acceptance research in the healthcare domain.

The survey utilised in this study aims to measure the ***perceived intention to adopt*** the proposed EHR system with IA measures for information management by future healthcare professionals. This scope is significant given that the implementation and operation of such a system will require a significant amount of time, resources and require extensive legislative support, which are only recently being initiated; for instance, in Australia (Further information related to the legal aspects of IA in healthcare is available in chapter seven).

The analysis of the results from the survey was conducted in two stages. Firstly a descriptive analysis was performed on the quantitative and qualitative data using IBM SPSS Version 19 (SPSS Inc, 2012). From the descriptive analysis, an assessment was made about the attitudes of the respondents towards the IAF characteristics. Secondly, the measurement model and the structural model were tested by focusing on the relationships of the model constructs and the hypotheses respectively. The partial least square (PLS) method of structural equation modelling (SEM) was used for this analysis. The analysis tool used was smartPLS 2.0 (Ringle, Wende, & Will, 2005).

3.2 METHODOLOGY AND RESEARCH MODEL DESIGN

Using existent theory to develop testable models of health information technology benefits both research and practice (Holden & Karsh, 2009). The research model designed and tested in this chapter draws from prior research in the field of technology acceptance in general, technology acceptance research in healthcare informatics and the findings from chapter two. The research model is primarily based on the UTAUT model (Venkatesh, et al., 2003) but is adopted to fit the survey cohort

and the IAF to be tested. Additional constructs have been introduced to measure the impacts of the IAF characteristics on the perceived intention to adopt the system.

3.2.1 Methodology

The method used in the study was a quantitative and qualitative questionnaire survey. The results presented in this chapter are of the first of a two phase survey which was designed and conducted to capture both the healthcare professionals' perspective and a patients' perspective on the IAF acceptance respectively following a successful pilot survey. The questionnaire was developed to capture well established technology acceptance constructs from previous research and the influence of the new characteristics introduced to the eHealth context by the IAF on those constructs together with the overall attitudes on the IAF characteristics. The primary goal of the survey was to assess the acceptability of the IAF in eHealth and the validation of a research model that can be used to measure technology acceptance of accountable-eHealth systems.

3.2.2 The Research Model Design

The UTAUT model has a high exploratory power resulting from its comprehensiveness and the care taken in its development (Schaper & Pervan, 2007). The research model shown in Figure 3.1 was designed to capture its already accepted relationships and was amended to fit the application context and the nature of the expected survey participants. The amendments also included previously untested constructs. A detailed account of the hypotheses is given in section 5.2.4.

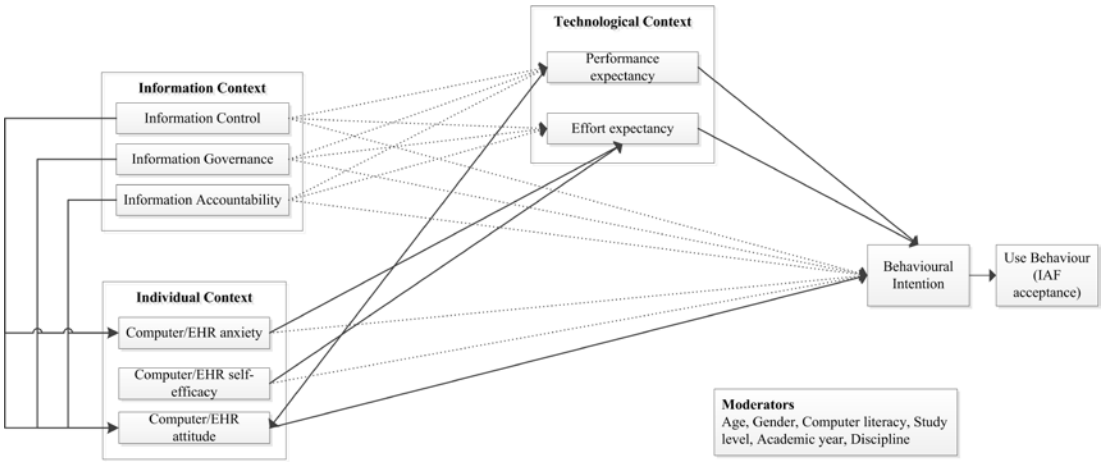


Figure 3.1 Hypothesised research model

3.2.3 The application of the UTAUT Model

The UTAUT model (Venkatesh, et al., 2003) was developed based on eight prominent technology acceptance models: the Technology Acceptance Model (TAM) (Davis, 1989), the Theory of Reasoned Action (TRA) (Fishbein & Ajzen, 1975), the Innovation Diffusion theory (IDT) (E. M. Rogers, 1995), the Theory of Planned Behaviour (TPB) (Ajzen, 1991), the Motivation Model (MM) (Davis, Bagozzi, & Warshaw, 1992), the Model of PC Utilisation (MPCU) (Thompson, Higgins, & Howell, 1991), the combined TAM and TPB (Taylor & Todd, 1995) and Social Congitive Theory (Compeau, Higgins, & Huff, 1999). UTAUT has four main constructs: performance expectancy, effort expectancy, social influence and facilitating conditions. The primary moderators of the model are gender, age, experience and voluntariness of use.

Although the model is applicable to a wide range of industries and disciplines including healthcare (Schaper & Pervan, 2007), its application in this study faced several limitations. Firstly, the survey participants were university students studying medicine, nursing or other health related courses. Although postgraduate students were within the cohort, the majority was undergraduate students. Therefore, constructs such as facilitating conditions were not included in the research model. Secondly, the type of eHealth system in question has not been implemented and the participants did not have a working experience of such a system. Determinants such as social influence therefore could not be included in to the research model.

3.2.4 Research Hypothesis

Technology acceptance in healthcare has been studied in the research domain for many years. Schaper et al. (2007) proposed a research model designed towards examining the ICT acceptance and utilisation by Australian occupational therapists. This model was based on the UTAUT model itself and a generic technology acceptance framework proposed by Chau et al. (2002b). They used three dimensions of technology acceptance: individual context, technology context and implementation context to capture the factors affecting the intention to use ICT. Together with the UTAUT model, we also focus on this work as a foundation for the designed research model presented here.

In our study, the hypotheses were formulated to capture both previously validated technology acceptance relationships and characteristics of the IAF. We adopt the individual context and the technology context constructs from Schaper et al. (2007) and introduce an information context, which deals with aspects relating to healthcare information manipulation within the IAF. The implementation context used by Chau et al. (2002b) and Schaper et al. (2007) were not utilised due to the specific focus and intention of the study being the perceived intention to use the proposed EHR system. A measure of the actual use of the system can only be measured once the proposed system can be implemented in a controlled healthcare setting, which at this stage of the study is not feasible given its complexity, limited resources and time constraints. The constructs used as measurements in each of the contexts are discussed next.

Individual context

Personal characteristics influence one's technology acceptance decisions (Chau & Hu, 2002b). As regards personal characteristics, many aspects have been previously studied under different circumstances. But, computer self-efficacy, computer anxiety and computer attitude are the most common and prominent constructs used in many technology acceptance studies (Venkatesh, et al., 2003). To be specific to the nature and domain of this study, we introduce "EHR" as an augmentation to the general meaning of "Computer" in this context, which is reflected in our hypotheses.

Computer Self-Efficacy is defined as the judgement of one's capability to use ICT (Compeau & Higgins, 1995). It can be applied, measured and described at a

general level or as pertaining to a specific application (Downey & McMurtrey, 2007; Marakas, Mun, & Johnson, 1998). Because this research model focuses on specific characteristics of a system, computer self-efficacy in used as a measure of the computer self-efficacy of a specific application.

Contrasting to other research (Compeau & Higgins, 1995; Compeau, et al., 1999; Hsu & Chiu, 2004; Igbaria & Iivari, 1995), the UTAUT model considered computer self-efficacy not to have a direct relationship to behavioural intention but to have an indirect effect being mediated by effort expectancy (Venkatesh, et al., 2003). Hence, we make the following hypotheses for our research model.

Hypothesis 1: Computer/EHR Self-Efficacy will have a direct positive effect on effort expectancy

Hypothesis 2: Computer/EHR Self-Efficacy will not have a direct effect on behavioural intention

Computer Anxiety is defined as an affective response of apprehension, or fear, when faced with the possibility of using ICT (Simonson, Maurer, Montag-Torardi, & Whitaker, 1987). Furthermore, according to Heinssen et al. (1987), computer anxiety involves a more effective response, such that resistance to and avoidance of computer technology are a function of fear and apprehension, intimidation, hostility, and worries that one will be embarrassed, look stupid or even damage the equipment. Factors such as erroneous beliefs of one's ability to use computers may be contributors to computer anxiety. Computer anxiety is said to have an effect on motivation and performance (Heinssen Jr, et al., 1987).

In the development of the UTAUT model, computer anxiety was modelled not to have a direct effect on behavioural intention but to have a direct effect on effort expectancy and thereby have an indirect effect on behavioural intention mediated by effort expectancy (Venkatesh, et al., 2003). Hence we formulate the following hypotheses relating to computer anxiety in our research model.

Hypothesis 3: Computer/EHR Anxiety will have a direct negative effect on effort expectancy

Hypothesis 4: Computer/EHR Anxiety will not have a direct effect on behavioural intention

Computer Attitude is an individual's overall affective reaction to using ICT (Venkatesh, et al., 2003). IT involves an individual's interest in and feelings of the enjoyment and pleasure that they feel with using ICT. Similar to computer anxiety, computer attitude is said to have an effect on motivation and performance of an individual when using ICT (Heinssen Jr, et al., 1987). In their study however, Venkatesh et al. (2003) found that computer attitude did not have a direct relationship towards behavioural intention, which was mediated by performance expectancy and effort expectancy. But in healthcare technology acceptance studies it was shown that computer attitude does in fact have a direct relationship with behavioural intention or technology acceptance (Chau & Hu, 2002b; Schaper & Pervan, 2007). Therefore we formulate the following hypothesis.

Hypothesis 5: Computer/EHR Attitude will have a direct positive effect on behavioural intention

Technological context

The perceptions of an individual's evaluation of technology has been found to have relevance in technology acceptance decision making in healthcare (Schaper & Pervan, 2007). In the technological context of this research model the focus is give to two constructs; performance expectancy and effort expectancy, which are theorised to have direct relationships to behavioural intention.

In the UTAUT model, **Performance Expectancy** is defined as the degree to which an individual believes that using the system will help him or her to attain gains in job performance (Venkatesh, et al., 2003). Being a very relevant construct in any technology domain, it has been established that performance expectancy is a significant aspect in the healthcare domain which has a direct effect in a health professionals' behavioural intention and an indirect effect to behavioural intention mediated by computer attitude (Chau & Hu, 2002b; Schaper & Pervan, 2007). Hence, we make the following hypotheses.

Hypothesis 6: Performance Expectancy will have a direct positive effect on behavioural intention

Hypothesis 7: Performance Expectancy will have a direct positive effect on computer attitude

Effort Expectancy as the degree of ease associated with the use of the system (Venkatesh, et al., 2003). In most technology acceptance literature, effort expectancy (mostly captured through *perceived ease of use* by Davis et al. (1989)) was found to have a direct relationship with behavioural intention. In contrast in the healthcare sector, studies have shown that effort expectancy does not have a significant influence on behavioural intention (Chau & Hu, 2002b; Chismar & Wiley-Patton, 2003; Jayasuriya, 1998). However, the study by Schaper et al. (2007) that utilised the UTAUT model, did establish that there is in fact a direct relationship of effort expectancy on behavioural intention (Schaper, 2009; Schaper & Pervan, 2007). The contrasting results may have been due to the specialised nature (Australian Occupational Therapists) of the participants in their study.

Given that this study is mostly based on the UTAUT model and that effort expectancy acts as a mediator for other constructs as theorised above, we will make the following hypothesis.

Hypothesis 8: Effort Expectancy will have a direct positive effect on behavioural intention

Information context

The information context has been introduced to the research model to capture the characteristics of the IAF and to measure the influence of those characteristics on acceptance of the proposed system. It consists of three main determinants; information control, information governance and information accountability. Each of these characterises the nature of the eHealth system that the user would use in a healthcare setting. Since the influence of these aspects has not been tested in prior research, we theorise that they may have an influence on all aspects of the research model that are logically sound. The IAF constructs may influence performance expectancy and effort expectancy. We also test their direct influence on behavioural intention. We assume that the new IAF capabilities will not have a negative effect on the acceptance of technology by healthcare professionals such that the introduction of those capabilities would not affect the overall acceptance of the EHR system.

We believe that the information context introduced here will play a significant role in the acceptance of technology in the healthcare domain. Because healthcare professionals have an expectation of timely availability and good quality information

and the facts that healthcare is driven by information, a significant focus should be given to how information is manipulated in the EHR system.

Information Governance is defined in this context as the enforcement of usage rules on how health professionals use a patients' healthcare information. These usage rules are captured by predefined purposes set by the health authority, which are discussed in detail in chapter five. The items in the information governance construct were designed to measure the attitudes of the participants towards the presence of information usage rules on how they can use patient information for healthcare purposes. The significance of this construct to the technological aspects is that it measures how this characteristic is perceived by the stakeholders. The influence of this aspect of the IAF is important given that misuse of information is initially detected using a knowledge base present in the IAF containing the purposes assigned for each data type in the EHR. Chapters five and six discuss these aspects in more detail.

We make the following hypotheses in regards to the information governance construct.

Hypothesis 9: *Information Governance will not have a direct negative effect on Effort expectancy*

Hypothesis 10: *Information Governance will not have a direct negative effect on Performance expectancy*

Hypothesis 11: *Information Governance will have a direct negative effect on Computer/EHR Anxiety*

Hypothesis 12: *Information Governance will have a direct negative effect on Computer/EHR Attitude*

Hypothesis 13: *Information Governance will not have a direct negative effect on behavioural intention*

The second construct in the information context is information control. It related to the characteristic of the IAF which gives patients the control of their healthcare information which is in accordance with eHealth requirements 6 and 7 given in section 1.2.6. **Information Control** is defined as the ability for the owner or subject of the information to control their healthcare information. Patient control of

healthcare information is a measure used to increase confidence in eHealth systems (Haas, et al., 2011). Allowing patients to set their own privacy rules to govern how healthcare professionals use their health information, although increases patient confidence and trust in the system, is not always beneficial to the patients. As discussed in chapter two, a patient is not always capable of deciding what data elements are required by a healthcare professional to make an informed decision. Although the IAF facilitate this capability, the process is overlooked by a healthcare authority to ensure that the healthcare process is unhindered by patient privacy policies. The perceptions the respondents have on information control thus directly relates to identifying how appropriate the related technological aspects given in chapters five and six would be if implemented in an eHealth system.

In our research model, we test the influence of this aspect of the IAF in the eyes of future healthcare professionals. We make the following hypotheses.

Hypothesis 14: *Information Control will not have a direct negative effect on Effort Expectancy*

Hypothesis 15: *Information Control will not have a direct negative effect on Performance Expectancy*

Hypothesis 16: *Information Control will have a direct negative effect on Computer/EHR Anxiety*

Hypothesis 17: *Information Control will have a direct negative effect on Computer/EHR Attitude*

Hypothesis 18: *Information Control will not have a direct negative effect on Behavioural Intention*

The final construct of the information context is **Information Accountability**. We measure the attitudes of future healthcare professionals towards holding healthcare professionals accountable and patients having the capability to inquire about possible misuse of information by a healthcare professional. This is directly related to eHealth requirement 8 in section 1.2.6. It also related to the characteristic of AeH systems which states that inappropriate use of information is followed by accountability (see section 2.8.1 in chapter two).

Similar to the previous constructs in the information context, we make the following hypotheses.

Hypothesis 19: *Information Accountability will not have a direct negative effect on Effort Expectancy*

Hypothesis 20: *Information Accountability will not have a direct negative effect on Performance Expectancy*

Hypothesis 21: *Information Accountability will have a direct negative effect on Computer/EHR Anxiety*

Hypothesis 22: *Information Accountability will have a direct negative effect on Computer/EHR Attitude*

Hypothesis 23: *Information Accountability will not have a direct negative effect on Behavioural Intention*

Behavioural intention

Behavioural intention was first introduced in the theory of reasoned action (TRA) (Fishbein & Ajzen, 1975). It is defined as the measure of the strength of one's intention to perform a specific behaviour (Fishbein & Ajzen, 1975). In technology acceptance research, behavioural intention was successfully used as a conclusive measure of the actual use of ICT by Davis (1989) in the Technology Acceptance Model (TAM). Since then, the relationship between behavioural intention and the actual use of ICT has been successfully established in technology acceptance research (Ajzen, 1991; Venkatesh & Davis, 2000; Venkatesh, et al., 2003). It is also the case in the healthcare context (Chau & Hu, 2002b; Chismar & Wiley-Patton, 2003). Therefore, considering the acceptance of the IAF as the actual use of ICT in our research model, we hypothesise that;

Hypothesis 24: *Behavioural Intention will have a direct positive effect on the acceptance of the IAF*

The survey hypotheses are summarised in Table 3.1.

Moderators

Moderating variables play a significant role in technology acceptance research (Schepers & Wetzels, 2007; H. Sun & Zhang, 2006). The main function of moderating variables is to explain the inconsistencies of the relationships between

constructs by identifying the situational differences (Chin, Marcolin, & Newsted, 2003). In technology acceptance models, the exploratory power is higher with the inclusion of moderating factors (Venkatesh, et al., 2003). In the UTAUT model, four moderating variables have been identified; age, gender, experience and voluntariness. Moderators such as computer literacy has been previously used in technology acceptance research in the healthcare domain together with others that are relevant to the application domain (Schaper & Pervan, 2007).

In our study, focusing on the nature of the participants, we consider six moderating variables; age, gender, computer literacy, academic year, level of study and discipline. Age and gender have been established in technology acceptance literature as to have effective moderating effects (H. Sun & Zhang, 2006; Venkatesh, et al., 2003). Although experience is a moderator of most technology acceptance studies (H. Sun & Zhang, 2006), in our research model, we theorise that the level of study, academic year and discipline to have a similar effect to experience.

Removal of constructs from UTAUT model

In the UTAUT model, social influence and facilitating conditions are also theorised and proved to have a significant contribution to behavioural intention and use behaviour respectively (Venkatesh, et al., 2003). Given the nature of the participants, those constructs were removed from this study. A student cohort is unlikely to be influenced by social factors and is not expected to have sufficient experience to be influenced by organisational facilitating conditions. We leave the utilisation of these two constructs to a future study involving healthcare professionals who will be able to work with a system implemented with the proposed IAF.

Table 3.1 Research hypotheses

Construct	Abbreviation	Hypothesis
Individual Context		
Computer self-efficacy	CSE	H1: CSE will have a direct effect on effort expectancy H2: CSE will not have a significant effect on behavioural intention
Computer (EHR) anxiety	ANX	H3: ANX will have a direct negative effect on effort expectancy H4: ANX will not have a direct negative effect on behavioural intention
Computer (EHR) attitude	ATT	H5: ATT will have a direct positive effect on behavioural intention
Technological Context		
Performance expectancy	PE	H6: PE will have a direct effect on behavioural intention H7: PE will have a direct effect on computer attitude
Effort expectancy	EE	H8: EE will have a direct effect on behavioural intention
Information Context		
Information governance	IG	H9: IG will not have a direct negative effect on Effort expectancy H10: IG will not have a direct negative effect on Performance Expectancy H11: IG will have a direct negative effect on Computer/EHR Anxiety H12: IG will have a direct negative effect on Computer/EHR Attitude H13: IG will not have a direct negative effect on behavioural intention

Information control	IC	H14: IC will not have a direct negative effect on Effort Expectancy H15: IC will not have a direct negative effect on Performance Expectancy H16: IC will have a direct negative effect on Computer/EHR Anxiety H17: IC will have a direct negative effect on Computer/EHR Attitude H18: IC will not have a direct negative effect on Behavioural Intention
Information accountability	IA	H19: IA will not have a direct negative effect on Effort Expectancy H20: IA will not have a direct negative effect on Performance Expectancy H21: IA will have a direct negative effect on Computer/EHR Anxiety H22: IA will have a direct negative effect on Computer/EHR Attitude H23: IA will not have a direct negative effect on Behavioural Intention
Acceptance of the IAF		
Behavioural Intention	BI	H24: BI will have a direct positive effect on the acceptance of the IAF

3.2.5 Survey items and constructs

The questionnaire items for each construct were either directly adopted from existing models (after adjusting to fit the cohort and application domain) or were designed specifically for the purpose of measuring the acceptance of the IAF by future healthcare professionals. The developed questionnaire items were verified by the rest of the research team and a qualified clinician and university lecturer involved with undergraduate teaching. Table 3.2 shows the questionnaire items for each of the constructs.

Table 3.2 Constructs and questionnaire items

Construct	Related hypothesis	Questionnaire item	Origin
Individual Context			
Computer self-efficacy (CSE)	H1 H2	CSE1….I would be able to complete different tasks without anyone around to tell me what to do CSE2….I would be able to complete tasks if I could call someone for help if I got stuck	Venkatesh et al., 2003
Computer/EHR anxiety (ANX)	H3 H4	ANX1….I feel apprehensive about using this EHR system ANX2….I would hesitate to use this EHR system for fear of making a mistake I cannot correct ANX3….I would be concerned about losing a lot of information by hitting the wrong key ANX4….I would find this EHR system intimidating	Venkatesh et al., 2003
Computer (EHR) attitude (ATT)	H5	ATT1….I believe that paper records can be better utilised to keep health information more secure than in EHRs ATT2….Using EHR systems is a good idea ATT3….I think EHRs are easy to work with than paper records	Developed to capture eHR attitude Venkatesh et al., 2003 Developed to capture eHR attitude

		ATT4….I think I would enjoy working with this EHR system ATT5….I think that EHR systems are expensive to implement and maintain. The expense could be better utilised to improve other healthcare facilities	Venkatesh et al., 2003 Developed to capture eHR attitude
Technological Context			
Performance expectancy	H6 H7	PE1….I believe that this EHR system would be useful in my professional activities PE2….I believe that this EHR would help improve my patient care delivery PE3….I think that this EHR system would improve my job performance PE4….I feel that this EHR system can make health information sharing easier and more effective	Venkatesh et al., 2003 Venkatesh et al., 2003 Developed to capture eHR attitude
Effort expectancy	H8	EE1….I think that learning to work with this EHR system would be easy EE2….I would find this EHR system easy to work with EE3….I believe I have or will develop the skills necessary to use this EHR system	Venkatesh et al., 2003 Venkatesh et al., 2003 Venkatesh et al., 2003
Information Context			
Information	H9 To H13	IG1….I believe that when health information is manipulated electronically (using computers), proper rules should be set	Developed to capture

Governance		on the use of health information IG2….I believe that when health information is manipulated electronically (using computers), a comprehensive knowledge base should govern information usage IG3….I believe that when health information is manipulated electronically (using computers), health professionals should be bound by predefined rules when using and accessing patient health information IG4….I believe that a health authority such as Queensland Health can formulate a comprehensive set of usage rules which indicate what health data is required for a given episode of care	attitudes towards having usage rules and a computerised knowledgebase
Information control	H14 To H18	IC1….I believe that patient participation (participatory medicine) in healthcare decision making is an important element in healthcare IC2….I believe that patients have the right to set their own privacy settings in an electronic health record system such as most social media websites IC3….I believe that patients have the right to decide which health professional can access his/her EHR	Developed to capture attitudes towards patients participation and control of health information
Information accountability	H19 to H23	IA1….I believe that if usage rules set by a health authority such as Queensland Health are broken intentionally, the offenders should be held accountable	Developed to capture the attitudes towards

		IA2….I think that patients have the right to inquire about possible misuse of their health information IA3….I think that health professionals should be required to justify why they have accessed/use information which they did not require for a given episode of care IA4….I feel that health professionals should be held accountable if found to have misused patient health information	accountability measures
Intention to Use			
Behavioural Intention	H24	BI1….I would use this EHR system in my professional activities for a few months BI2….I would use this EHR system throughout my professional career	Venkatesh et al., 2003

3.3 PARTICIPANTS

3.3.1 Selection criteria

Participants were selected such that a wide range of potential healthcare professionals are involved in the study so that the results are more generalisable. The selection of the participants purely depended on the availability of the resources and the willingness of the participating institutions.

Quantitative data as well as qualitative data in the form of comments to specific questions from university students of three universities were collected using an online survey tool. The selection of the universities and the student cohort depended purely on their availability and the willingness of the institutions to participate in the survey. The participants ranged from medical students to health sciences students. The distribution of participants across each institute is shown in Figure 3.2.

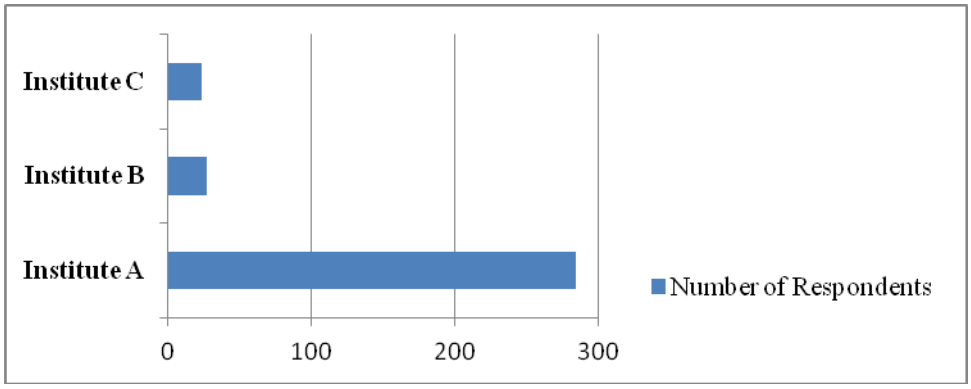


Figure 3.2 Distribution of participants across participating institutes

The number of respondents from institute B and C are low compared to institute A due to the fact that only medical students from those institutes were invited to participate. Institute A did not have a medical school; therefore, all health related students were invited to participate.

3.3.2 Participants from institution A

The participants from institute A comprised on undergraduate and post graduate students studying health sciences including nursing, optometry, pharmacology etc. The participant attributes are listed in Table 3.3.

Table 3.3 Respondents from Institute A

		Nursing (n)		Other (n)		
		Male	**Female**	**Male**	**Female**	**Total**
Bachelors	**1st year**	3	24	15	47	206
	2nd year	1	13	2	28	
	3nd Year	3	15	7	23	
	4th year	0	4	1	19	
	Graduated	0	0	0	1	
Masters	**1st year**	1	4	3	5	32
	2nd year	0	2	2	7	
	3nd Year	0	1	1	1	
	4th year	0	0	0	0	
	Graduated	0	0	0	5	
PhD	**1st year**	0	1	1	1	9
	2nd year	0	0	0	1	
	3nd Year	0	0	0	1	
	4th year	0	1	0	2	
	Graduated	0	0	0	1	
Other	**1st year**	1	3	2	9	37
	2nd year	1	2	0	1	
	3nd Year	0	2	0	1	
	4th year	0	0	2	4	
	Graduated	1	3	0	5	
Notes: Study level categorised as other include diploma, certificate, graduate certificate and graduate diploma.						284

The age of the respondents ranged from 17 years to a maximum of 58 with mean 27 (SD = 10.55). The age distribution of the participants is shown in Table 5.4.

Table 3.4 Age range of respondents

Age Range (years)	Number of respondents
17-20	103
21-30	89
31-40	40
41-60	49

3.3.3 Participants from institution B

The participants from institution B comprised of undergraduate medical students. The participant attributes are listed in Table 3.5. The age of the respondents ranged from 20 years to 43 years with a mean of 25.67(SD = 4.59).

Table 3.5 Respondents from Institution B

	Male	Female
1st year	4	3
2nd year	1	4
3nd Year	1	3
4th year	4	7
Total	10	17

3.3.4 Participants from institution C

The participants from institution C comprised of postgraduate students studying medicine, nursing and other health related courses. The participant attributes are listed in Table 3.6.

Table 3.6 Respondents from Institution C

		Medicine		Nursing		Other		
		Male	Female	Male	Female	Male	Female	Total
MSc	1st year	0	1	0	0	0	1	15
	2nd year	0	0	0	1	1	2	
	3nd Year	1	1	0	0	0	0	
	4th year	0	0	0	1	0	1	
	Graduated	2	2	0	0	0	1	
PhD	1st year	0	0	0	0	3	0	8
	2nd year	0	2	0	0	0	0	
	3nd Year	0	0	0	1	0	0	
	4th year	0	0	0	1	0	0	
	Graduated	0	1	0	0	0	0	

Note: Participants categorised as "Other" include pharmacology, radiation therapy, sports health, human services, nutrition and dietetics, biomedical science, psychology, social work, medical science, paramedics, public health optometry and psychiatry

The age of respondents ranged from a minimum of 22 years to a maximum of 51 years with a mean age of 32.78 (SD = 7.49).

3.4 THE SURVEY

3.4.1 Instrument

The survey questions were included in an online survey tool and were formatted such that the readability and presentation of the survey was appropriate. Questions were distributed in such a way that the ceiling and floor effects were minimal. The survey was distributed via email invitation to all prospective participants (see Appendix B for email invitation). Because all university students were already familiar with email and Internet technologies, there were no hindrances

expected from the use of an online survey tool in terms of usability. The online survey distribution and response collection was also expected to maximise the response rate.

3.4.2 Survey Administration

A detailed description was given to the participants outlining the specific characteristics of the EHR system, similar to Angst and Agrawal's (2009) approach. Rather than testing the participants' knowledge about EHRs, as done by Angst and Agrawal (2009), given the participants' education background related to healthcare, we assumed they had a basic understanding of EHRs. The survey questions were designed to further outline the characteristics specific to the IAF such as policy setting by patients and inquiries and justifications. The survey specifically noted that the questions were related to EHRs and the newly introduced information accountability measures. The questions focused on the attitudes the respondents had on an EHR system designed using the IA principles. A screen capture of the first page of the survey tool can be found in Appendix C.

After the participating institutions agreed for the survey to be launched within specific areas of the institutions, email invitations were sent to the expected participants by the respective authorities. The survey was also included in an internal newsletter at institution C. After four weeks time of the launch of the survey, a reminder email was sent to all participants at institution A. Data collection was terminated after a total of 6 weeks.

3.4.3 Ethics and Limitations

Ethical clearance was obtained from the authors' education institution to conduct the research study, which did not include any health and safety issues. From the other two participating institutions, one institution required ethical clearance, which was obtained before the study commenced. There were no ethical issues or incidents arising from this study. The ethical clearance certificates can be found in Appendix A.

As previously stated, the study was limited to a student population from the three different educational institutions. Professional institutions and societies within the healthcare domain were initially contacted to include participants for the research but the requests were denied due to their resource limitations and busy time

schedules of healthcare professionals. A decision was made afterwards to include a suitable student cohort that would deliver a limited but similar result to what could have been expected from current healthcare professionals. This was done so that the research study could be completed within the available time frame.

3.5 DESCRIPTIVE ANALYSIS OF THE RESULTS

In order to present the overall acceptability of the IAF by the survey participants, a descriptive analysis of the results was performed and is presented in this section. A descriptive analysis of the results is also required to establish the practical significance of the research questions. It is a means of multivariate analysis of the results based on their substantive findings rather than statistical significance (Hair, Anderson, Tatham, & Black, 1998). The analysis software used for the descriptive analysis was IBM SPSS Version 19 (SPSS Inc, 2012).

3.5.1 Response

A total of 334 valid responses were received as a result of an initial email request and reminder emails broadcasted over the respective faculties and schools in the participating institutions. The responses also include qualitative data acquired through unrestricted comments.

3.5.2 Analysis

The questions asked from the participants are categorised in to 9 variables which are also used to test the measurement model, structural model and hypotheses. A total of 31 items were used to measure the variables. An additional six questions were also asked from the participants regarding the EHR system in question. The model variables, the individual items and the mean and standard deviation of each item and variable are shown in Table 3.7. The percentage response of each item is also given.

Table 3.7 Descriptive data of questionnaire items relating to the measurement model

	Strongly Disagree		%		Strongly Agree		
	1	**2**	**3**	**4**	**5**	**Mean**	**SD**
Computer/EHR self efficacy						**3.81**	**.79**
CSE1	0.9	8.4	35.0	41.9	13.8	3.59	.86
CSE2	0.9	2.7	10.8	63.2	22.5	4.04	.72
Computer/EHR anxiety						**2.42**	**1.03**
ANX1	15.0	47.0	16.2	19.5	2.4	2.47	1.04
ANX2	16.2	47.0	12.3	20.7	3.9	2.49	1.11
ANX3	14.7	43.1	10.5	26.3	5.4	2.65	1.17
ANX4	21.6	58.1	12.6	7.5	0.3	2.07	.81
Computer/EHR attitude						**3.69**	**.94**
ATT1*	3.3	22.2	15.9	45.8	12.9	3.43	1.07
ATT2	1.2	2.4	18.0	49.7	28.7	4.02	.82
ATT3	1.2	7.8	14.4	45.2	31.4	3.98	0.94
ATT4	0.6	5.1	24.3	48.2	21.9	3.86	.84
ATT5*	6.9	17.4	35.6	32.6	7.5	3.16	1.03
Performance expectancy						**3.96**	**0.84**
PE1	0.6	4.8	13.2	47.9	33.5	4.09	0.84
PE2	0.6	6.6	19.8	44.3	28.7	3.94	0.89
PE3	1.2	7.8	29.9	43.4	17.7	3.69	.89
PE4	0.6	1.8	12.6	56.3	28.7	4.11	.73
Effort expectancy						**3.96**	**.76**
EE1	0.9	6.0	25.7	50.6	16.8	3.76	.83
EE2	0.9	3.9	28.7	48.2	18.3	3.79	0.81
EE3	0.0	0.6	6.9	53.0	39.5	4.31	.63
Information governance						**4.21**	**.76**
IG1	0.0	0.0	5.4	35.0	59.6	4.54	.59
IG2	0.0	1.2	14.4	49.4	35.0	4.18	.71
IG3	0.0	1.2	6.9	40.1	51.8	4.43	.68
IG4	4.2	10.2	21.9	40.4	23.4	3.69	1.07
Information control						**3.75**	**1.02**
IC1	0.0	3.0	6.3	47.6	43.1	4.31	.72
IC2	6.9	24.0	19.2	30.5	19.5	3.32	1.23
IC3	5.7	16.8	14.7	35.9	26.9	3.62	1.21
Information accountability						**4.36**	**.74**
IA1	0.0	1.5	10.8	41.3	46.4	4.33	.73
IA2	0.3	1.2	3.0	39.5	56.0	4.50	.65
IA3	2.1	5.1	8.1	48.5	36.2	4.12	.91
IA4	0.6	0.3	6.0	36.5	56.6	4.48	.68
Behavioural intension						**3.50**	**.91**
BI1	1.2	8.4	34.7	43.1	12.6	3.84	.79
BI2	0.0	3.0	31.4	43.7	21.9	3.16	1.03
Notes * reverse coded item							

Computer/EHR self-efficacy

The item means of all items used to measure CSE was greater than the midpoint of the scale, the overall mean score being 3.81 (0.79). This indicates that

the respondents believed they were able to use the proposed EHR system confidently. But this indication was not very strong but significantly favourable towards the proposed system.

Computer/EHR anxiety

The level of anxiety the respondents showed was low in the sense that the means of all items used to measure ANX was lower than the midpoint of the scale. But, with an overall mean score of 2.42 (1.03), the respondents' computer anxiety was not very low.

Computer/EHR attitude

All the items used to measure ATT showed individual means greater than the midpoint of the scale and ATT showed an overall mean score of 3.69 (0.94). Although the respondents' attitude towards the EHR system is favourable it is not very high.

Performance expectancy

PE had an overall means score of 3.96 (0.84) with the means of all individual measurement items being higher than the midpoint of the scale. This indicates that the participants believed that by using this EHR system, their professional performance will be enhanced. The indication is at a significantly good level.

Effort expectancy

Similar to PE, EE had an overall means score of 3.96 (0.76) with all indicator mean scores higher than the midpoint of the scale. This indicates that the participants believed that a high degree of ease is associated with using the EHR system. This is a favourable indication of positive acceptance of the IAF.

Information governance

The overall mean score for IG was 4.21 (0.76). This is a very strong indicator that the respondents believed that usage rules are an important factor in the EHR system. Although above the midpoint of the scale, IG4 had the lowest mean score of 3.69 indicating that the respondents' confidence in the capability of a central authority to formulate usage rules was not as high as the other indicators. This may be because the question mentioned the name of the local healthcare authority and at the time of data collection there were a number of issues raised against it.

Information control

IC showed an overall mean score of 3.75 (1.02). All indicators showed a mean score of above the midpoint of the scale. Respondents believed that patient participation in the healthcare proves and making decisions about their health information is important. As expected, over 50% of respondents felt very strongly that patient consent is critical before using health information, but they were least confident about patient setting their own privacy rules with only 19.5% of them choosing the highest scale item.

Information accountability

IA showed a very high overall mean score of 4.36 (0.74). Every item used to measure the accountability aspect had a mean score significantly above 4.0. The respondents strongly believe that accountability measures are needed in EHR systems. This is a strong indicator of the significance of the IAF in healthcare.

Behavioural intension

The respondents indicated that they desire to use this EHR system is high with an overall mean score of 3.50 (0.91). Both of the items used to measure BI had a mean score over 3.0. The higher of the two was for BI1 indicating that they would use the system for a few months of their professional activities. In terms of the intention to use a future EHR system, a score of 3.50 can be considered to be strong.

Overall response

The overall response to the questionnaire items indicates that the respondents' felt favourably towards the characteristics of the designed EHR system. Therefore the overall acceptance of the proposed EHR system with the technological aspects presented in chapters five and six is favourable.

Apart from the measurement model construct reported above, additional questions were asked from the participants regarding the EHR system.

Table 3.8 Additional questionnaire items

Theme	Strongly Disagree		%		Strongly Agree	
Information availability	**1**	**2**	**3**	**4**	**5**	**Mean (SD)**
I would prefer to have access to information that is only related to the current episode of care.	19.2	50.3	12.9	14.4	3.3	**2.32 (1.04)**
I would require complete access to a patients' health record without any access restrictions.	4.8	26.9	20.1	32.6	15.6	**3.27 (1.16)**
Information sharing	**1**	**2**	**3**	**4**	**5**	**Mean (SD)**
I believe that care givers should be allowed to share patient information with other professionals.	4.5	14.1	19.5	51.5	10.5	**3.49 (1.01)**
Privacy concerns	**1**	**2**	**3**	**4**	**5**	**Mean (SD)**
I believe that storing and managing health information electronically (using computers) in this EHR system will hinder patient privacy.	8.7	41.9	21.9	22.2	5.4	**2.74 (1.07)**
I feel that patient information, even with personal identifiable information removed, should not be accessed by any outside entity or authority for any reason other than the caregiver(s) for the purpose of providing healthcare.	5.1	25.7	11.4	29.6	28.1	**3.50 (1.28)**

The respondents are more favourable towards having unrestricted access to health information than being limited to a specific set of information. But the indication is not very strong. The respondents' attitudes are favourable towards information sharing and believe that sharing should be allowed. The respondents believe that this EHR system poses no threat to information privacy issues and believe that information should only be used for the purpose of healthcare. But, secondary use of healthcare information is important in some cases to enhance the delivery of care such as in research.

3.5.3 Qualitative data analysis

At the end of the survey the participants were asked to comment on the proposed EHR system and its accountability features. A total of 70 written responses

were received. Following are some of the comments and interpretations categorised under themes relevant to the study. Table D.1 in Appendix D summarises the comments received from the respondents regarding different aspects of the EHR system. The comments given by respondents have been assessed and categorised in to 6 themes, Data access/availability, Accountability measures/Information misuse, Patients control, Attitudes on overall system, Attitudes towards EHR/eHealth and other.

The respondents have a strong belief that healthcare professionals should have access to as much information about a patients' medical status as possible in order to make a well informed decision towards the wellbeing of the patient. They feel apprehensive about patients being able to set their own privacy rules but believe that patient privacy is paramount. Some believe that EHR all together could hinder confidentiality. In their perspective, the patient-physician relationship should be built around trust.

The majority of the respondents feel that they and their patients would benefit from EHR systems in general. But some claim that paper records would still dominate over electronic health records. The main negative concerns of the respondents around EHR systems are mainly based on unauthorised access to the systems resulting from poor security measures. Computer literacy has also been stated as a barrier for EHR system adoption. Some negative bias to EHR systems from some respondents can be observed resulting from previous experience with the local healthcare authority.

The respondents strongly believe that information misuse should be followed by appropriate penalties for the relevant users to enforce accountability. One respondent stated that,

"*…overall I am for the idea, just don't like the idea that patients will restrict the type of information I can access. How is a patient to know if past medical history is relevant or not? I feel like I would like to know everything possible about the patient in order to give them the best possible care - however if patients are able to see which information I access, I would be hesitant to do so, in case it attracts litigation.*"

The aim of accountable-eHealth systems as discussed in chapter two is to deter users from misusing information, which this comment highlights. With the assurance that legitimate use of information would not result in legal action and since the respondent is in favour of the system she has a high tendency to adopt the system.

The respondents feel that information should only be used for the purposes for which they have been collected. This strong belief is a positive aspect towards the future acceptability of an IAF in the eHealth domain. Further support to the proposed EHR system can be observed from the respondents' comments. But, issues such as usability are mentioned in the comments indicating that they are concerned about how the system would be delivered to the end users. Overall the qualitative data indicates a favourable attitude from the respondents towards the proposed EHR system with the IA characteristics discussed in chapter two.

3.6 ASSESSMENT OF THE RESEARCH MODEL AND HYPOTHESIS TESTING

The assessment of the research model was conducted using the partial least square (PLS) method of structural equation modelling (SEM). PLS was developed to maximise prediction rather than fit; to maximise the proportion of the variance of the dependent construct that is explained by the predictor constructs. PLS is particularly suitable for data analysis during the early stages of theory development where the theoretical model and its measures are not well formed (Tsang, 2002). The PLS analysis follow a two-step method involving the evaluation of the results of the measurement model and the assessment of the structural model.

3.6.1 Assessment of the measurement model

The reliability and validity of the model constructs and the items used to measure the constructs were evaluated by the assessment of the measurement model. The properties of the measurement model were assessed using *construct reliability* and *discriminant and convergent validity* techniques in PLS.

Construct reliability

The construct reliability is a measure of the construct to determine to what extent an individual can answer the same question the same manner each time (Detmar Straub, 1989). Construct reliability in PLS is determined by using individual

item reliability, internal consistency and the average variance extracted (AVE) (Barclay, Higgins, & Thompson, 1995).

Individual item reliability

PLS was used to test the internal consistency by producing individual item loading for each construct. Hair et al. (1998), as cited by Igbaria et al. (1997), state that individual item reliability is considered significant if the loading is greater than 0.3 (Igbaria, et al., 1997) and that the significance increases thereafter. Only one item out of the 31 items used to measure the constructs has a loading less than 0.3. An item used to measure information control, IC1, had a loading of (-0.089). This item was removed from further analyses. The resulting item loadings are shown in Table 3.9.

Table 3.9 individual item loadings

Construct	Indicators	Loading
Computer/EHR self-efficacy (CSE)	CSE1	0.8975
	CSE2	0.6632
Computer/EHR anxiety (ANX)	ANX1	0.8003
	ANX2	0.8064
	ANX3	0.6822
	ANX4	0.778
Computer/EHR attitude (ATT)	ATT1	0.8511
	ATT2	0.6907
	ATT3	0.7032
	ATT4	0.636
	ATT5	0.8521
Performance expectancy (PE)	PE1	0.8445
	PE2	0.848
	PE3	0.7001
	PE4	0.802
Effort expectancy (EE)	EE1	0.7385
	EE2	0.8424
	EE3	0.8532
Information governance (IG)	IG1	0.7643
	IG2	0.7827
	IG3	0.7358
	IG4	0.6402
Information control (IC)	IC2	0.6025
	IC3	0.6473
Information accountability (IA)	IA1	0.8244
	IA2	0.6534
	IA3	0.463
	IA4	0.7773
Behavioural intention (BI)	BI1	0.6685
	BI2	0.9244

Internal consistency and average variance extracted (AVE)

Using the same PLS results which produced the previous results, internal composite reliabilities were produced as a determinant of the internal consistency. All internal composite reliabilities were greater than 0.707, which is the threshold for acceptable reliability (Igbaria, et al., 1997).

Finally the average variance extracted (AVE) was measured to determine the amount of variance a construct captures from its indicators relative to the amount due

to measurement error (Chin, 1998). All constructs showed an AVE of greater than the 0.5 threshold. Results are shown in Table 3.10.

Table 3.10 Internal composite reliabilities and average variance extracted

Construct	AVE	Composite Reliability
Computer/EHR self-efficacy (CSE)	0.6227	0.7635
Computer/EHR anxiety (ANX)	0.5904	0.8516
Computer/EHR attitude (ATT)	0.5653	0.8651
Performance expectancy (PE)	0.6414	0.8767
Effort expectancy (EE)	0.6610	0.8535
Information governance (IG)	0.5371	0.8219
Information control (IC)	0.5424	0.7742
Information accountability (IA)	0.5030	0.7808
Behavioural intention (BI)	0.6507	0.7841

Discriminant and Convergent Validity

Discriminant and convergent validity are measures of construct validity. Discriminant validity is used to measure the difference of a construct to other constructs used in the model (Schaper, 2009). Convergent validity is used to determine the convergence of the items used to measure a construct. It shows how they associate with each other to reflect the construct they are designed to measure (Datmar Straub, M. C. Boudreau, & Gefen, 2004). In PLS, correlations of the constructs and cross loading of constructs are used to determine the discriminant and convergence validity.

Correlation of constructs

In the measurement of correlation of constructs, the square root of AVE must be greater than the correlation with other constructs (Datmar Straub, et al., 2004). Table 3.11 shows the correlation of constructs with the square root of AVE (shown in bold).

Table 3.11 Correlation of constructs and square root of AVE

	CSE	ANX	ATT	PE	EE	IG	IC	IA	BI
CSE	**0.789**								
ANX	-0.326	**0.768**							
ATT	0.372	-0.569	**0.751**						
PE	0.335	-0.480	0.792	**0.801**					
EE	0.410	-0.564	0.557	0.498	**0.813**				
IG	0.310	-0.224	0.306	0.333	0.280	**0.732**			
IC	0.003	0.106	-0.072	-0.04	-0.059	0.222	**0.736**		
IA	0.163	-0.199	0.169	0.167	0.133	0.520	0.288	**0.709**	
BI	0.310	-0.415	0.610	0.666	0.388	0.259	-0.092	0.126	**0.806**

Only one item (PE) was found to have a slightly higher value than the square root of AVE of ATT. The correlation of performance expectancy and computer/EHR attitude can be expected because the model exhibits a causal relationship amongst them. Overall, discriminant and convergent validity is acceptable.

Cross loadings of constructs

Cross loadings of constructs reveal the fit of individual items load on the latent variable compared to their loadings on other variables (Schaper, 2009). Table 3.12 presents the cross loadings of the constructs, which revealed that the loadings for each of the indicators are significantly higher than those of the other constructs. We come to the conclusion that the discriminant validity of the model indicators is acceptable because the indicators used reflect the constructs they are designed to reflect than other constructs.

Table 3.12 Cross loading of constructs

Indicators	CSE	ANX	ATT	PE	EE	IG	IC	IA	BI
CSE1	**0.897**	-0.319	0.306	0.267	0.392	0.276	0.016	0.091	0.230
CSE2	**0.663**	-0.170	0.2956	0.28	0.231	0.2087	-0.021	0.2009	0.2876
ANX1	-0.321	**0.800**	-0.616	-0.594	-0.504	-0.322	-0.006	-0.273	-0.449
ANX2	-0.260	**0.806**	-0.412	-0.338	-0.383	-0.122	0.0959	-0.100	-0.329
ANX3	-0.134	**0.682**	-0.284	-0.165	-0.331	-0.074	0.1436	-0.071	-0.190
ANX4	-0.240	**0.778**	-0.352	-0.261	-0.475	-0.099	0.1409	-0.11	-0.242
ATT1	0.1773	-0.400	**0.6360**	0.3743	0.2955	0.1401	-0.095	0.0745	0.3559
ATT2	0.2913	-0.422	**0.8521**	0.7816	0.4677	0.2914	-0.045	0.1677	0.5758
ATT3	0.3095	-0.366	**0.7032**	0.5000	0.4558	0.1629	-0.047	0.1189	0.4119
ATT4	0.3574	-0.494	**0.8511**	0.7019	0.5743	0.3068	-0.003	0.1499	0.4938
ATT5	0.2442	-0.478	**0.6907**	0.5145	0.2511	0.2021	-0.114	0.1002	0.4145
PE1	0.2702	-0.383	0.6513	**0.8445**	0.4078	0.2478	-0.021	0.1215	0.556
PE2	0.2135	-0.352	0.614	**0.8480**	0.3825	0.2395	-0.017	0.1181	0.5347
PE3	0.2913	-0.388	0.6763	**0.8020**	0.4355	0.2331	0.0002	0.0817	0.5662
PE4	0.2966	-0.412	0.5899	**0.7001**	0.3634	0.3515	-0.112	0.2198	0.4695
EE1	0.3276	-0.439	0.4340	0.3908	**0.8424**	0.2092	-0.041	0.0654	0.2396
EE2	0.356	-0.418	0.4691	0.4306	**0.8532**	0.2165	0.006	0.0844	0.3259
EE3	0.3121	-0.504	0.4479	0.3866	**0.7385**	0.2506	-0.101	0.163	0.364
IG1	0.2516	-0.180	0.1884	0.1962	0.2069	**0.7643**	0.1685	0.4264	0.2122
IG2	0.235	-0.191	0.2343	0.289	0.1935	**0.7827**	0.1494	0.3864	0.1912
IG3	0.1508	-0.175	0.0987	0.1168	0.1206	**0.7358**	0.2486	0.5281	0.1161
IG4	0.2335	-0.118	0.3022	0.3008	0.2533	**0.6402**	0.1231	0.2558	0.204
IC2	0.0400	0.0698	0.0156	0.0223	-0.024	0.1107	**0.6025**	0.1973	0.0012
IC3	0.0422	0.0451	-0.030	-0.011	0.0338	0.0905	**0.6473**	0.2144	-0.068
IA1	0.164	-0.175	0.1749	0.1414	0.132	0.4985	0.1868	**0.8244**	0.1267
IA2	0.0856	-0.100	0.0829	0.1264	0.0674	0.2907	0.3124	**0.6534**	0.0523
IA3	-0.017	-0.011	-0.009	0.0310	-0.026	0.2861	0.3599	**0.4630**	-0.021
IA4	0.1087	-0.166	0.1109	0.1156	0.0934	0.352	0.1887	**0.7773**	0.0948
BI1	0.2631	-0.160	0.3014	0.3463	0.2166	0.2012	-0.075	0.1157	**0.6685**
BI2	0.2581	-0.444	0.6187	0.6667	0.3809	0.2259	-0.078	0.1004	**0.9244**

3.6.2 Assessment of the structural model

Assessment of the structural model reveals the significance of the hypotheses in the model. The process involves testing the predictive power of the model and the significance of the relationships between the models' constructs (Schaper, 2009).

Predictive properties of the model

The predictive power of the model was established by performing PLS analysis. R2 values of the entire model were produced and for each of the dependent variables. The results are show in Table 3.13.

Table 3.13 Predictive properties of the model

Construct	R^2 Value
Computer/EHR attitude (ATT)	0.630
Computer/EHR anxiety (ANX)	0.069
Effort expectancy (EE)	0.378
Performance Expectancy (PE)	0.069
Behavioural intention (BI)	**0.473**

The results revealed that the model was capable of predicting 47.3% of the behavioural intention of the participants towards the acceptance of the IAF. The predictive power of the model is a highly satisfactory level in technology acceptance research. The model was also able to predict 63.0% of variance in computer/EHR attitude, 6.9% of variance of computer/EHR anxiety, 37.8% of variance in effort expectancy, and 6.9% of that in performance expectancy.

Relationship between model constructs

To establish the relationship of the model constructs, the path coefficients and t-values for each of the structural model paths were calculated. Seventeen of the 18 hypotheses are tested here. From the available technology acceptance literature we assume a direct relationship between BI and actual use behaviour contributing to the acceptance of the IAF.

A bootstrapping resampling technique was used to calculate the values using smartPLS. The analysis used 100 randomly selected samples from the 334 cases. The corresponding p-values were determined using an F-distribution table and the values are given in Table 3.14.

Table 3.14 t-value and corresponding p-value

t-value	p-value
$t > 1.96$	$p < 0.05$
$t > 2.57$	$p < 0.001$
$t > 3.29$	$p < 0.0001$

The results of the bootstrapping and PLS analysis are summarised in Figure 5.3 and Table 3.15.

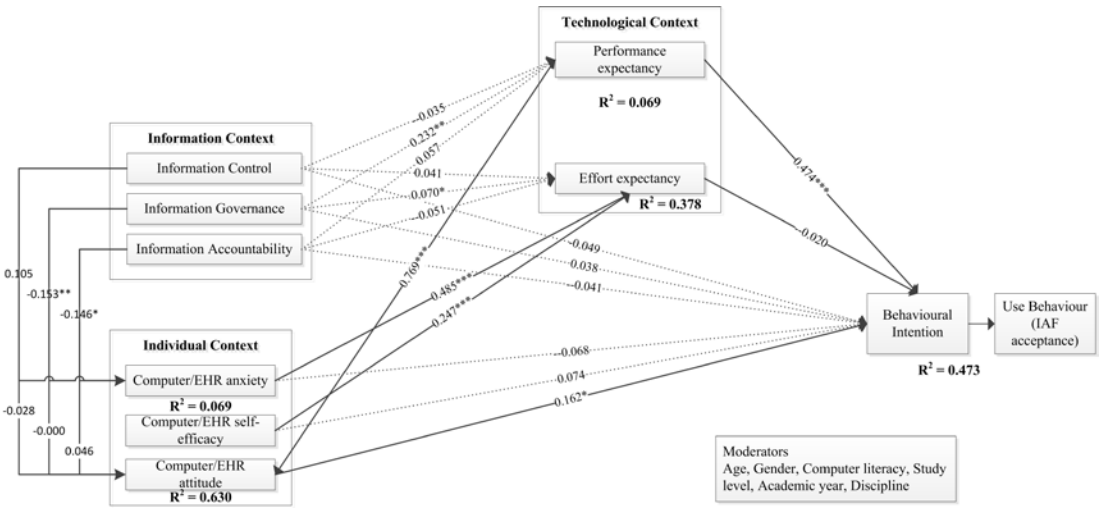


Figure 3.3 Results of the structural model

The relationships shown in dotted lines in Figure 3.3 are relationships initially hypothesised to be non-significant.

Table 3.15 Individual path significance

Path	t-Statistics	Path Coefficients	Hypothesis
CSE → EE	4.9404**	0.2474	H1
CSE ↛ BI	1.4122	0.0735	H2
ANX → EE	8.558***	-0.4853	H3
ANX ↛ BI	1.243	-0.0681	H4
ATT → BI	2.0758*	0.1624	H5
PE → ATT	30.3758***	0.7691	H6
PE → BI	7.828***	0.4739	H7
EE → BI	0.341	-0.0203	H8
IG ↛ EE	2.145*	0.070	H9
IG ↛ PE	5.755**	0.232	H10
IG → ANX	2.665**	-0.153	H11
IG → ATT	0.006	-0.000	H12
IG ↛ BI	0.6823	0.038	H13
IC ↛ EE	0.736	0.041	H14
IC ↛ PE	0.562	-0.035	H15
IC → ANX	1.541	0.105	H16
IC → ATT	0.751	-0.028	H17
IC ↛ BI	1.179	-0.049	H18
IA ↛ EE	0.969	-0.051	H19
IA ↛ PE	0.823	0.057	H20
IA → ANX	2.279*	-0.146	H21
IA → ATT	0.997	0.046	H22
IA ↛ BI	0.0507	-0.041	H23

Notes
*p < 0.05, **p < 0.01, ***p < 0.001

The PLS analysis revealed that seven hypotheses were not supported (H8, H9, H10, H12, H16, H17 and H22). Effort expectancy, as discussed earlier, is associated with the degree of ease of using a system. By not having a significant effect on behavioural intention, it supports previous technology acceptance research in the healthcare domain (Chau & Hu, 2002b; Chismar & Wiley-Patton, 2003; Jayasuriya, 1998).

IG and IA showed significant negative effects on ANX, thus supporting hypotheses H11 and H21 respectively. This negative relationship indicates that if a

respondent feels that either accountability measures or computerised information governance are suitable, their anxiety level about the system reduces and vice versa. From the descriptive analysis of the results in section 3.5, we observed a favourable attitude towards these constructs from the respondents indicating that the respondents' anxiety levels are not heightened by the presence of these measures. However, despite the fact that IA and IG negatively affect ANX, since there is no significant effect from ANX on BI, their effect on BI is not significant. IG had significant positive effects on PE and EE. This indicates that if a respondent believes that the presence of a computerised knowledgebase that governs usage is suitable, it would improve their perceived job performance and perceived ease of use. Since we saw from the descriptive analysis in section 3.5 that respondents are favourable towards the IG aspects, the designed EHR system characteristic in regards to IG, which is technologically feasible through the purpose definitions discussed in chapter five, is suitable for implementation. Our hypotheses H13, H18 and H23 were also supported from the results, which indicate that the presence of usage rules on health information use, accountability measures and the fact that patients have control of their information does not negatively affect BI. We believe that this is a favourable outcome towards the implementation of AeH systems and the technological aspects presented in chapters five and six.

Two of the three hypothesised direct effects on behavioural intention were found to be statistically significant (PE and ATT) while performance expectancy had the highest direct effect (with path coefficient = 0.4739***). In general, technology acceptance research finds that attitude does not have a significant effect on behavioural intention (Venkatesh, et al., 2003). But in the healthcare sector, computer attitude has been seen to have a significant effect on behavioural intention (Chau & Hu, 2002b), supporting our findings.

The indirect effects may also contribute to the total effect on behavioural intention. We calculate the indirect effects of each on the constructs on behavioural intention. The total effect of a construct to behavioural intention is the sum of the direct and indirect effects. The indirect effect of a construct to behavioural intention can be calculated by multiplying the relevant structural coefficients along the path (Igbaria, et al., 1997).

Table 3.16 Total effects on behavioural intention

Construct	Total effect
Computer/EHR self efficacy	0.0706
Computer/EHR anxiety	-0.0605
Computer/EHR attitude	0.1685*
Performance expectancy	0.6064***
Effort expectancy	-0.0162
Information governance	0.1858***
Information control	-0.0814
Information accountability	0.0379

As presented in Table 3.16, the strongest direct effect on behavioural intention was from performance expectancy followed by information governance and computer/EHR attitude. The model showed that none of the information context constructs had a negative effect on the attitudes of the participants in adopting the proposed EHR system in their professional activities, which is a positive outcome for the IAF, especially in terms of information governance.

3.6.3 Influence of moderating variables on the structural model

Moderating factors have a significant role in technology acceptance research (H. Sun & Zhang, 2006). Six factors were theorised to have moderating effects on the research model by considering the characteristics of the participants. Age, gender, computer literacy, study discipline, academic year and study level (e.g. undergraduate level, master's level, PhD level, etc.) were selected as moderating factors. Age and gender are key factors in the UTAUT model whilst year of study and study level were used to replace experience.

Due to the presence of the new constructs in the research model, which are previously untested, and with the available data set, it is not possible to test specific hypotheses for the moderating variables. However, the theorised moderating factors were tested to examine their impact on the relationships between the model constructs and also the exploratory power of the model. With the knowledge of gained from this study, a future study involving active healthcare professionals can be done to further test the impact of the moderating variables with specific hypotheses.

In order to perform the statistical analysis for each of the moderating variables, separate data sets were created for each category of each moderating variable using SPSS Version 19. Table 3.17 summarises the distribution of the data set in to each category. The following series of tables summarise the PLS and bootstrapping calculations performed on each of the new datasets.

Table 3.17 Moderating variable categories

Moderating variable	Category	Number of cases
Gender	Male	64
	Female	270
Age (years)*	17 - 20	104
	21 - 30	125
	31-60	102
Computer literacy	Excellent	167
	Good	134
	Moderate	33
Study Discipline**	Medicine	43
	Nursing	85
	Other	196
Year of Study***	First year	96
	Second year	49
	Third year	52
	Forth year or graduated	36
Study Level	Undergraduate	231
	Postgraduate	103

Note: * Age had three missing values; *** Study Discipline had 10 missing values;
** Only the year of study of the undergraduate students was considered

Gender

The following table shows the path coefficients of the moderating variable Gender. The ratio of male to female respondents is 1:4 as shown in table 3.17. Therefore we expect the influence of the female respondents on the research model to be more significant.

Table 3.18 Path coefficients of moderating variable Gender

	Gender	
	Male	***Female***
ATT - R^2	0.5824	0.6491
EE - R^2	0.4838	0.3919
ANX - R^2	0.0895	0.0846
PE - R^2	0.0876	0.1339
BI - R^2	0.5103	0.4764
Path coefficients with significance		**Hypothesis**
CSE → EE	0.2015*	0.2274***	H1
CSE ↛ BI	0.0863	0.0644	H2
ANX → EE	-0.6105***	-0.4497***	H3
ANX ↛ BI	0.1574	-0.1181	H4
ATT → BI	0.236	0.1712*	H5
PE → ATT	0.6848***	0.7991***	H6
PE → BI	0.467***	0.4684***	H7
EE → BI	0.1495	-0.0538	H8
IG ↛ EE	-0.16	0.2046**	H9
IG ↛ PE	0.1183	0.3576***	H10
IG → ANX	-0.209	-0.152*	H11
IG → ATT	-0.045	0.048	H12
IG ↛ BI	0.128	0.027	H13
IC ↛ EE	0.1229	0.0448	H14
IC ↛ PE	-0.084	-0.0167	H15
IC → ANX	-0.052	0.137*	H16
IC → ATT	-0.090	-0.015	H17
IC ↛ BI	-0.0191	-0.0272	H18
IA ↛ EE	0.137	-0.1247**	H19
IA ↛ PE	0.2146	0.0191	H20
IA → ANX	-0.0130	-0.181**	H21
IA → ATT	0.195	0.011	H22
IA ↛ BI	-0.084	-0.0215	H23

Notes:
1. *p<0.05; **p<0.001; ***p<0.0001
2. The hypotheses shown in red are unsupported hypotheses from the entire sample

The results of the PLS analysis of the separate data sets for gender are shown in Table 3.18. In the male sample of 64 respondents, only hypotheses H5, H10 and H21 were found to be contradicting to the original findings. In the female sample of 270 respondents, hypotheses H16 and H19 were contradictory to the original findings. The female sample exhibit more sensitiveness to the newly introduced information context constructs relating to the IAF characteristics but does not have a

significant effect on the behavioural intention. Although these results are satisfactory, a balanced overall sample can be used to measure to reach a more conclusive decision on the moderating effects of gender.

Age

Table 3.19 shows the path coefficients of the moderating variable Age.

Table 3.19 Path coefficients of moderating variable Age

	Age			
	17-20	***21-30***	***31 - 60***	
ATT - R^2	0.6051	0.6618	0.5866	
EE - R^2	0.4959	0.3815	0.3918	
ANX - R^2	0.0802	0.0741	0.0469	
PE - R^2	0.1245	0.193	0.0658	
BI - R^2	0.5902	0.4761	0.467	
Path coefficients with significance				**Hypotheses**
CSE → EE	0.279***	0.2147*	0.1725	H1
CSE ↛ BI	0.2267**	0.0585	-0.0632	H2
ANX → EE	-0.5166***	-0.4657***	-0.5094***	H3
ANX ↛ BI	-0.0935*	-0.1164	-0.0748	H4
ATT → BI	0.324	0.0226	0.2254*	H5
PE → ATT	0.7471***	0.8215***	0.7206***	H6
PE → BI	0.3341**	0.5498***	0.4779***	H7
EE → BI	-0.0942	-0.0014	-0.0457	H8
IG ↛ EE	0.271**	0.1654	0.0687	H9
IG ↛ PE	0.1139	0.4449***	0.2203	H10
IG → ANX	-0.930	-0.187*	-0.137	H11
IG → ATT	-0.148*	0.073	0.118	H12
IG ↛ BI	0.0314	0.0044	0.1024	H13
IC ↛ EE	0.1237	0.1014	-0.0186	H14
IC ↛ PE	-0.1122	0.1095	-0.1299	H15
IC → ANX	0.187	0.065	0.080	H16
IC → ATT	-0.018	-0.023	-0.010	H17
IC ↛ BI	-0.1129	-0.1159	0.1074	H18
IA ↛ EE	-0.1812	-0.1683	0.0813	H19
IA ↛ PE	0.2649	-0.0633	0.0361	H20
IA → ANX	-0.158	-0.136	-0.117	H21
IA→ ATT	0.158	-0.058	0.053	H22
IA ↛ BI	-0.0659	0.1226	-0.0246	H23

Notes:
1. *p<0.05; **p<0.001; ***p<0.0001
2. The hypotheses shown in red are unsupported hypotheses from the entire sample

The results of the PLS analysis of the data sets for the separate age categories are shown in Table 3.19. Respondents were categorised in to three groups depending on their age; 17 to 20 (n = 104), 21 to 30 (n = 125), 31 to 60 (n = 102). The intervals were chosen in such a way so that their sample size were over 60 for the PLS analysis. In terms of the original hypotheses results, the first age group contradicts the findings for H2, H4, H4, H9, H10, H11 and H21; the second age group contradicts the findings for H5 and H21 and the third group contradicts the results for H1, H11 and H21. The results converge to the original findings when age increases. The significance of CSE on EE and BI reduced with age where older respondents showing no significance. Whilst younger respondents showed no significance of ATT to BI, respondents aged between 31 and 60 showed a significance relationship with ATT and BI. We conclude that age has a significant moderating effect on the attitudes of respondents towards the IAF.

Computer literacy

The following table shows the path coefficients of moderating variable computer literacy. The respondents were asked to rate their computer skill on a 5-point scale (Excellent, Good, Moderate, Poor and Very Poor). None of the respondents indicated that their computer literacy was either poor or very poor. This can be expected from a student population. Therefore, those levels were discarded.

Table 3.20 Path coefficients of moderating variable Computer Literacy

	Computer Literacy			
	Excellent	***Good***	***Moderate***	
ATT - R^2	0.6585	0.6146	0.5242	
EE - R^2	0.3393	0.3279	0.4199	
ANX - R^2	0.0826	0.045	0.1261	
PE - R^2	0.1111	0.07	0.2242	
BI - R^2	0.5569	0.3683	0.6605	
Path coefficients with significance				**Hypotheses**
CSE → EE	0.2385**	0.1819	0.1226	H1
CSE ↛ BI	0.1368	-0.057	0.0871	H2
ANX → EE	-0.389***	-0.5115***	-0.5048***	H3
ANX ↛ BI	-0.0671	-0.112	0.0175	H4
ATT → BI	0.0653	0.2331	0.1667	H5
PE → ATT	0.8053***	0.7773***	0.7374***	H6
PE → BI	0.5823***	0.3691**	0.4413	H7
EE → BI	-0.0203	-0.0403	0.0642	H8
IG ↛ EE	0.1811*	0.1278	0.0369	H9
IG ↛ PE	0.3065**	0.2843*	0.3492	H10
IG → ANX	-0.165	-0.018	-0.100	H11
IG → ATT	0.067	-0.030	0.0178	H12
IG ↛ BI	0.0833	-0.1091	0.4331**	H13
IC ↛ EE	0.0976	-0.014	0.2717	H14
IC ↛ PE	-0.0439	-0.0158	0.2106	H15
IC → ANX	0.044	0.130	0.052	H16
IC → ATT	0.014	-0.028	-0.104	H17
IC ↛ BI	-0.0329	-0.0717	-0.2167	H18
IA ↛ EE	-0.1172	-0.1102	0.0024	H19
IA ↛ PE	0.0512	-0.0368	0.056	H20
IA → ANX	-0.170	-0.193	-0.310	H21
IA → ATT	-0.007	-0.061	-0.017	H22
IA ↛ BI	-0.0965	0.1249	-0.2704	H23

Notes:
1. *p<0.05; **p<0.001; ***p<0.0001
2. The hypotheses shown in red are unsupported hypotheses from the entire sample

The subsamples of computer literacy were categorised in to Excellent (n = 167), Good (n = 134) and Moderate (n = 33). All three categories supported the original findings relating to all hypotheses except for H1, H5, H11 and H21. But the results from the "Moderate" group are not conclusive given that the number of respondents was less than the required minimum of 60. We also note that because the

distribution was severely skewed towards computer literacy levels being high (because the majority of the participants can be considered digital natives), the results are not entirely generalisable. But there was no significant negative effect on the intention to adopt the system from the IAF characteristics. Given that the range of computer literacy was not adequate, a final conclusion cannot be reached regarding the moderating effects of computer literacy from the results from the current data set.

Discipline

Table 3.21 shows the path coefficients of moderating variable Discipline. The main disciplines were Medicine (n = 43) and Nursing (n = 85).

Table 3.21 Path coefficients of moderating variable Discipline

	Discipline		
	Medicine	***Nursing***	***Other***
ATT - R^2	0.7441	0.6723	0.6069
EE - R^2	0.5429	0.4885	0.3619
ANX - R^2	0.2772	0.2424	0.0367
PE - R^2	0.1563	0.3172	0.0693
BI - R^2	0.5934	0.5667	0.4663
Path coefficients with significance			**Hypotheses**
CSE → EE	0.177	0.1701	0.2364**	H1
CSE ↛ BI	0.3775	-0.1826	0.1142	H2
ANX → EE	-0.564***	-0.4813***	-0.4755***	H3
ANX ↛ BI	-0.0575	-0.0653	-0.1152	H4
ATT → BI	0.1422	0.3854*	0.0978	H5
PE → ATT	0.8516***	0.8009***	0.7604***	H6
PE → BI	0.3505	0.4163**	0.4861***	H7
EE → BI	0.1209	-0.0488	-0.036	H8
IG ↛ EE	-0.1112	0.2793*	0.0962	H9
IG ↛ PE	0.1804	0.6207***	0.2186**	H10
IG → ANX	-0.524	-0.320**	-0.083	H11
IG → ATT	0.050	0.112	0.023	H12
IG ↛ BI	-0.133	0.0736	0.0244	H13
IC ↛ EE	0.2714*	0.1601	0.0198	H14
IC ↛ PE	0.1876	0.0073	-0.0895	H15
IC → ANX	-0.116	0.298**	0.023	H16
IC → ATT	0.029	-0.127	-0.078	H17
IC ↛ BI	-0.3035	0.1316	-0.0966	H18
IA ↛ EE	-0.0575	-0.0243	-0.0924	H19
IA ↛ PE	0.1068	-0.112	0.0662	H20
IA → ANX	0.103	-0.072	-0.141	H21
IA → ATT	-0.035	-0.038	0.047	H22
IA ↛ BI	0.1258	0.0053	0.0177	H23

Notes:
1. *p<0.05; **p<0.001; ***p<0.0001
2. The hypotheses shown in red are unsupported hypotheses from the entire sample

The third category (n = 196) categorised as "*Other*" consists of respondents from Optometry, Pharmacology, Psychiatry, and several other health science disciplines. The moderating effect of these categories was not measured individually because of their low individual sample sizes (n < 60). The results revealed that the all three groups support the original results relating to all hypotheses except for H1, H5,

H7, H9, H10, H11, H16 and H21. Medical students seem to be less influenced by the information context than nursing students who show sensitiveness to IG. But, there is no evidence, in all three categories, indicating negative effects by the IAF characteristics towards behavioural intension. Note that the number of medical students was less than 60, indicating that the respective results are not entirely conclusive.

Level of study

Table 3.22 shows the path coefficients of moderating variable Level of Study. The data set was divided in to two categories depending on the level of study; undergraduate level (n = 231) and postgraduate level (n = 103). Postgraduate level respondents include Master's level, PhD level, graduate diploma and graduate certificate level students.

Table 3.22 Path coefficients of moderating variable Level of Study

	Level of Study		
	Undergraduate	***Postgraduate***	
ATT - R^2	0.6577	0.5942	
EE - R^2	0.4226	0.3892	
ANX - R^2	0.0963	0.0802	
PE - R^2	0.1145	0.1298	
BI - R^2	0.5385	0.4097	
Path coefficients with significance			**Hypotheses**
CSE → EE	0.2747***	0.0962	H1
CSE ↛ BI	0.0739	0.0809	H2
ANX → EE	-0.4753***	-0.5391***	H3
ANX ↛ BI	-0.0936	0.0293	H4
ATT → BI	0.2241*	0.061	H5
PE → ATT	0.8056***	0.7007***	H6
PE → BI	0.4251***	0.5835***	H7
EE → BI	-0.0216	0.0121	H8
IG ↛ EE	0.1782*	0.0597	H9
IG ↛ PE	0.2846**	0.3643**	H10
IG → ANX	-0.103	0.223	H11
IG → ATT	-0.010	0.133	H12
IG ↛ BI	0.0386	-0.0328	H13
IC ↛ EE	0.0874	-0.0288	H14
IC ↛ PE	-0.064	-0.008	H15
IC → ANX	0.162**	0.005	H16
IC → ATT	-0.051	0.034	H17
IC ↛ BI	-0.1017	0.052	H18
IA ↛ EE	-0.1379*	0.0833	H19
IA ↛ PE	0.0913	-0.0058	H20
IA → ANX	-0.238**	-0.093	H21
IA → ATT	0.018	0.164	H22
IA ↛ BI	0.0414	-0.0354	H23

Notes:
1. *p<0.05; **p<0.001; ***p<0.0001
2. The hypotheses shown in red are unsupported hypotheses from the entire sample

Results from the two subsamples supported most of the original results relating to the hypotheses. Postgraduate students did not exhibit a significant effect on EE from CSE whilst with undergraduate students it was very significant. Similarly, ATT had a significant effect on BI with undergraduate students but not with postgraduate students. The effect of the IAF characteristics (H9 and H15) was higher in

undergraduate students than with postgraduate students who showed no significant effect on their intention to use the system. Overall, there was no significant negative effect on the intention to use the proposed system by either group. But there is a clear moderating effect on the model from level of study.

Academic year

Table 3.23 shows the path coefficients of moderating variable Academic year. Due to the fact that postgraduate students who responded to the survey may have had prior industry exposure of some nature, the academic year of only the Undergraduate level respondents was considered as a moderating factor.

Table 3.23 Path coefficient of moderating variable Academic Year

	Academic Year				
	First	***Second***	***Third***	***Fourth***	
ATT - R^2	0.6542	0.6702	0.6863	0.7057	
EE - R^2	0.4363	0.4023	0.4664	0.5154	
ANX - R^2	0.1693	0.2022	0.2375	0.2636	
PE - R^2	0.2229	0.2066	0.1296	0.2098	
BI - R^2	0.5199	0.7119	0.4885	0.678	
Path coefficients with significance					**Hypotheses**
CSE → EE	0.3012***	0.3064*	0.2364	0.2029	H1
CSE ↛ BI	0.0216	0.2571*	0.1081	0.0611	H2
ANX → EE	-0.4859***	-0.401**	-0.47**	-0.5478	H3
ANX ↛ BI	-0.1321	-0.017	-0.1299	-0.1435	H4
ATT → BI	0.2224	0.4333*	0.1493	0.0552	H5
PE → ATT	0.8***	0.8181***	0.7646***	0.8036***	H6
PE → BI	0.4851***	0.1201	0.4378	0.6992**	H7
EE → BI	-0.0467	0.0247	0.0589	-0.1369	H8
IG ↛ EE	0.2561*	0.1731	0.1753	-0.1373	H9
IG ↛ PE	0.3552**	0.3352**	0.2268	-0.4494	H10
IG → ANX	-0.092	-0.165	-0.284	0.452	H11
IG → ATT	-0.017	0.002	0.015	-0.151	H12
IG ↛ BI	-0.0119	0.2025	-0.1609	-0.0411	H13
IC ↛ EE	0.1083	-0.0418	0.0118	-0.065	H14
IC ↛ PE	0.1146	-0.1395	-0.1779	-0.1353	H15
IC → ANX	0.112	0.024	0.330*	0.239	H16
IC → ATT	-0.081	0.007	-0.140	-0.006	H17
IC ↛ BI	-0.0664	-0.196*	0.0611	-0.1508	H18
IA ↛ EE	-0.2749**	-0.0519	-0.0826	0.2622	H19
IA ↛ PE	0.1117	0.1125	0.1812	0.0614	H20
IA → ANX	-0.375*	-0.338	-0.191	-0.052	H21
IA → ATT	0.078	0.009	0.132	0.082	H22
IA ↛ BI	-0.0082	0.0143	0.0538	0.1223	H23

Notes:
1. *p<0.05; **p<0.001; ***p<0.0001
2. The hypotheses shown in red are unsupported hypotheses from the entire sample

The subsamples were populated such that 96 first year students, 49 second year students, 52 third year student and 36 fourth year students were present in each category. Note that three of the categories have respondents less than the required sample size of 60. The results may not be entirely conclusive.

The results mostly support the original findings from the entire data set. The effects of the IAF characteristics although significant in some cases (H9, H10, H18, H19 and H21) with first and second year students become insignificant factors with the third and fourth year students. Overall there were no negative effects from the IAF characteristics towards the intention to use the proposed system, supporting the original results. The academic year exhibited a noticeable moderating effect on the model.

Measuring the effects of the moderating factors allows for a further clarification of the original results by identifying the situational differences (Chin, et al., 2003). In this study, we have seen that the moderating factors indeed affect the model paths. Although a considerable effect on R^2 by every moderator was observed, its effects are said to be modest (Chin, et al., 2003). Important to this research, we have established that with the results from the moderating factor analysis that there are no negative effects from the introduced IAF characteristics towards the participants' intention to adopt and use the proposed EHR system, which is a favourable outcome for the rest of the study.

3.7 DISCUSSION AND CONCLUSION

In this chapter we have surveyed a medical and health science student cohort and measured their attitudes towards an EHR system augmented with information accountability principles for better information management as presented in chapter two to investigate how such a system would be accepted by future healthcare professionals. We have also developed, tested and validated a new empirical research model that is suitable to measure the perceived intention to use AeH systems by using previously accepted technology acceptance theories.

The initial step of the investigation was a descriptive analysis of the survey results. The results from the descriptive analysis of the quantitative and qualitative data suggest that such a system would be favourably accepted by future healthcare professionals. As we saw in section 3.5, the respondents' attitudes towards the system were high and their anxiety levels were low. We have seen from chapter two that information accountability in the healthcare domain is important and relevant for appropriate information privacy management. Although a strong attitude towards patient privacy is present, the respondents are mainly concerned about the timely and

comprehensive access to healthcare information, which was identified through eHealth requirement 2 in section 1.2.6. The respondents attitudes towards specific systems characteristics such as patients having control of their healthcare information, being bound by predefined rules for information usage and the possibility of being held accountable for misuse of information were also favourable, which are technologically feasible through what is discussed in chapters five and six.

The next step of the investigation was to identify how different aspects, be it technical or psychological, influence the intention to adopt the proposed system. We conceptualised a research model from existent technology acceptance theories that can be empirically tested from the survey results. To test the research model, we measured 9 constructs of which 6 were adopted from previously accepted technology acceptance models and three were newly introduced to capture the characteristics of the IAF in eHealth, which are directly related to the technological presented in chapters five and six. Twenty four relationships were hypothesised between the constructs and 23 were tested using the survey data. The final hypothesis was theorised to be significant from previous research.

The assessment of the measurement model and structured model was done using the partial least square (PLS) approach of structural equation modelling (SEM). Construct reliability measurements showed that one item user to measure the information control construct had unacceptable reliability. This item was removed from further analysis. The model exhibited acceptable internal consistency (> 0.7) for each construct indicating that the model was both valid and reliable.

The PLS results revealed that the model was capable of predicting 47.3% of the variance of behavioural intention towards acceptance of the IAF. A PLS analysis with bootstrapping was performed to test the 23 hypotheses. Seven out of the 23 hypotheses tested were not supported. In technology acceptance research, effort expectancy was shown to have a significant positive effect on behavioural intention. Contrastingly though in the healthcare domain, this was disproven in several studies, as was the case in this study. Information governance was hypothesised not to have a negative effect on effort expectancy and performance expectancy. But unexpectedly in this study, it showed a significant positive effect on both.

As indicated earlier, the information context constructs are designed to capture AeH system characteristics and a direct association can be made with the case

scenario given in section 2.6 in chapter two. Information control relates to Patient X's capability to nominate the healthcare professionals he/she want to be able to have access to his/her EHR and the fact that custom access policies (reflecting information privacy requirements) can be set for them by Patient X. Information governance relates to StateHealth defining healthcare access policies that govern the access to healthcare information and the definition of intended purposes for data access. As stated in the case scenario, certain relationships are present between data types and they are maintained by StateHealth, which adds to the intended purposes. Information accountability is related to the fact that healthcare professionals can be held accountable for inappropriate use of information. In our scenario, if Dr. B had accessed Patient X's mental health details he would have been asked to justify why the action occurred. Dr. B's justification may or may not be valid depending on the circumstances. Our survey respondents felt strongly that this characteristic is important to EHR systems, which is clear from that descriptive analysis of the quantitative and qualitative data presented in section 3.5. More detailed descriptions of the AeH system characteristics that were measured from the information context constructs are given in chapters five and six.

The effects of moderating factors on the model constructs were also tested. We found that age, gender, study discipline, study year and the level of study had moderating effects on the research model. Because the moderating variable computer literacy was severely skewed, generalisable conclusions could not be made. We believe that further studies are required to test the extent to which each moderating factor effect the model.

The only contributing factor found to have an effect on system acceptance was computer/EHR attitude and performance expectancy. Although the information context constructs had no significant positive direct effects (except IG on EE and PE) there were no negative effects on any of the other constructs. However, we did observe a significant positive total effect of IG on BI. This means that the additional accountability characteristics do not negatively affect EHR adoption. Overall we conclude that, when accountable-eHealth (AeH) systems are implemented, they will be favourably accepted by the future healthcare professionals.

Having established the above conclusion from the results obtained, we point out that the representativeness of the data set is not entirely general to all healthcare

professionals. For example, only a limited number of medical students were surveyed. We propose a future study involving healthcare professionals with varied levels of experience with EHR systems to further validate the findings of this study.

Chapter 4: Views on Information Accountability in eHealth: The Consumers' Perspective

In this chapter, we present the results of a survey conducted to measure the attitudes of the general consumers towards information accountability in eHealth. A research model and descriptive analysis of survey data are presented. The quantitative and qualitative data utilised in this chapter originated from 187 completed survey responses from university student studying non-health related courses at the Queensland University of Technology, Brisbane, Australia. The survey investigates how the concepts behind the information accountability framework (IAF) designed for eHealth systems would be accepted by future eHealth consumers. The results from the survey analysis support the applicability IA principles in the eHealth domain. The findings indicate that there is support from the consumers' perspective for the technological aspects of the IAF reported in chapters five and six. Research objective 4(b) is addressed in this chapter.

4.1 INTRODUCTION

The lack of consumer adoption is one of the main impediments to eHealth. This related to both healthcare professionals as well as the general consumers, i.e. patients or individuals who own an EHR. Low consumer adoption of technology can be seen as a critical issue in many eHealth initiatives around the world. This was recently evident in Australia relating to the PCEHR system (Barlass, 2012). The main concern for consumers is privacy and security of their health information. Although there is ample evidence and concerns pertaining to the technology perspective relating to security and privacy in eHealth (Petkovic & Ibraimi, 2011), there are only a few studies conducted in that regards (Or & Karsh, 2009; Wilkowska & Ziefle, 2011). Most of the studies conducted in relation to patients attitudes are focused on consumer health information technologies, i.e. computer-based systems that are designed to facilitate information access and exchange, enhance decision making, provide social and emotional support, and help behaviour changes that promote health and well-being (Gustafson et al., 2002; Or & Karsh, 2009). The

attitudes of the consumers towards EHR systems that enable them to manage their own healthcare information have not been extensively researched. But in recent eHealth developments, a significant degree of these types of systems are being developed. It is therefore important to measure the attitudes of the consumers towards eHealth systems and system attributes which directly affects system acceptance once implemented.

Consumers may see an increased opportunity to use EHR systems because they empower consumers to participate in information sharing and decision making, which enables them to be more in control and contribute to quality healthcare (Or & Karsh, 2009). But their acceptance of these technologies is hindered by several reasons. Poor availability, lack of training, lack of computer skills and low self-efficacy can be seen as several major reasons. Relevant to EHR system, which manage sensitive health information, information privacy, security and trust issues also contribute to the low adoption rate. There is evidence to suggest that the lack of adoption of eHealth technologies by the consumers has led to the failure of a number of eHealth projects (Jimison et al., 2008; A. Rogers & Mead, 2004; Stoop, van't Riet, & Berg, 2004; P. Williams, Nicholas, & Huntington, 2003).

The focus of this chapter is given to the consumers' perspective on a newly designed measure (the IAF) to address information privacy. It is stated that the understanding of factors that influence technology acceptance is essential for its successful adoption (E. M. Rogers, 1995). The influence of technology acceptance has been extensively studied, most commonly, in the business arena. Although technology acceptance research has been done in the healthcare domain as reported in chapter three, very little work is done pertaining to the patients' perspective (Korzaan & Boswell, 2008; Wilkowska & Ziefle, 2011). But, the knowledge about the attitudes of patients towards eHealth systems is needed to ensure that the design of future systems will be acceptable to patients (Whiddett, Hunter, Engelbrecht, & Handy, 2006b).

The term "acceptance" has been previously defined in several ways in the prominent technology acceptance literature (Or & Karsh, 2009). The main four ways it has been defined are: the satisfaction with the technology; use or adoption of the technology; efficient or effective use of the technology; and the intention or willingness to use the technology (Chau & Hu, 2002a, 2002b; Davis, 1989; Karsh,

2004; Venkatesh, et al., 2003; Whitten & Richardson, 2002). The last definition of acceptance is the focus of this study.

This chapter presents the results of a survey and a conceptual research model developed by considering facts presented in chapter two to measure the acceptance of the IAF in eHealth by eHealth consumers. A descriptive analysis of the survey data is presented as a measure of the perceived attitudes towards the IAF. Similar to what was done in chapter three the research model is based on well established technology acceptance model constructs and their relationships together with constructs and relationships hypothesised to be significant in the study domain. Many of the same constructs used in chapter three are utilised in this chapter. However, since the study is measuring the consumers' perspective as opposed to the professionals' perspective, the perception for the same construct may be different, i.e. opposite to what was observed in chapter three. Therefore the hypotheses in this chapter are made accordingly.

The survey utilised in this study aims to measure the ***perceived intention to adopt*** the proposed EHR system with IA measures for information management by potential consumers of the system, i.e. patients. This scope is significant given that the implementation and operation of such a system will require a significant amount of time, resources and require extensive legislative support, which are only recently being initiated, for instance, in Australia (refer to chapter seven for more details about the legal aspects related to IA in healthcare).

The analysis of the results from the survey followed the methods used in chapter three. Firstly, a descriptive analysis was performed on the quantitative and qualitative data using IBM SPSS Version 19 (SPSS Inc, 2012). From the descriptive analysis, an assessment was made about the attitudes of the respondents towards the IAF characteristics. Secondly, the measurement model and the structural model were tested focusing on the relationships of the model constructs and hypotheses respectively using partial least square (PLS) analysis. The PLS analysis tool used was smartPLS 2.0 (Ringle, et al., 2005).

4.2 METHODOLOGY AND RESEARCH DESIGN

The research model design in this chapter follows the same method used in chapter three. The research model used to test the attitudes of the general public was

designed based on published technology acceptance research and research relating to people's attitudes towards eHealth technologies. In the design of the relationships between specific aspects (constructs), consideration is also given to the findings from chapter three. Previously untested constructs are introduced to the research model to capture the IAF characteristics similar to what was done in chapter three.

4.2.1 Methodology

The method of research was a quantitative and qualitative questionnaire survey. The results resented in this chapter is the final part of the two part survey which was designed and carried out to capture patients' attitudes towards the designed EHR system with IA characteristics. The questions included in the questionnaire were either adopted from previous technology acceptance research or have been developed specifically for this study. The primary goals of this chapter are; firstly, to measure how the designed EHR system would be accepted in the future by the members of the general public and secondly, to validate the research model used in the study using the survey data.

4.2.2 Research model design

Chapter three established three main contexts which influence the behavioural intention to use technology that relates to the acceptance of the IAF in eHealth. In this section of the study, two of the three contexts are brought forward and an additional context is introduced to the research model. The individual context, the information context, and the privacy context are theorised to have influence on the behavioural intention of patients towards accepting the designed IAF. Figure 4.1 shows the designed research model.

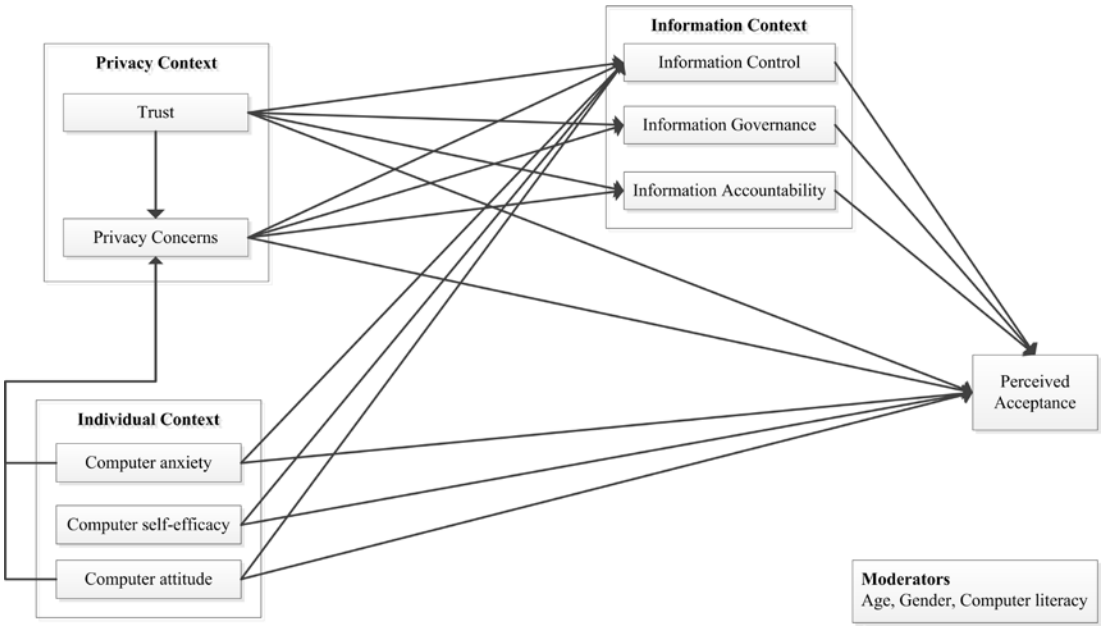


Figure 4.1 Hypothesised research model

The main hypotheses made here relate to the relationships between the model constructs within the information context and privacy context to determine their role in the perceived attitude of the respondents towards accepting the IAF.

4.2.3 Research Hypothesis

The hypotheses for this research study were based on technology acceptance research in general and in the healthcare domain focusing on the consumers' acceptance of technology. The hypotheses are related to the structural relationships amongst the model constructs. Each of the three contexts and their related hypotheses are discussed in this section.

Individual context

Similar to what was discussed in chapter three, for the individual context we consider three constructs; computer self-efficacy (CSE), computer anxiety (ANX) and computer attitude (ATT). These constructs are drawn from the unified theory of acceptance and use of technology (UTAUT) (Venkatesh, et al., 2003).

Previous studies that tested consumer acceptance of health ICT acceptance, the usability characteristics of a technology, a person's feelings, perceptions, or beliefs about a technology can affect their perceived acceptance of that technology (Holden & Karsh, 2009). Therefore, the aforementioned constructs are used to capture

different aspects in relation to the above. Formal definitions or meanings of each of the constructs can be found in chapter five.

Results from chapter five and the UTAUT model (Venkatesh, et al., 2003) showed that **Computer Self-Efficacy** does not have a direct relationship with behavioural intention. But, other research on consumer acceptance of technology in the healthcare domain has shown that CSE is in fact a predictor of acceptance (Compeau & Higgins, 1995; Hsu & Chiu, 2004; Hu, Chau, Sheng, & Tam, 1999). In this study, CSE can also be theorised to have a direct effect on information control, a capability given to the consumers for self control of their healthcare information by the IAF. The considerations resulted in the following hypotheses.

Hypothesis 1: Computer/EHR Self-Efficacy will have a direct positive effect on the consumers' perception on information control

Hypothesis 2: Computer/EHR Self-Efficacy will have a direct effect on the consumers' perceived acceptance of the technology

Although **Computer Anxiety** was found to be only indirectly related to behavioural intention in technology acceptance research involving professionals (Schaper & Pervan, 2007; Venkatesh, et al., 2003), consumer related studies in the healthcare domain has found a direct relationship between ANX and behavioural intention (Finkelstein, Khare, & Ansell, 2003; Lai, Larson, Rockoff, & Bakken, 2008; Lober et al., 2006), which directly related to acceptance. Computer anxiety has also been theorised to have a direct negative effect on privacy concerns (Korzaan & Boswell, 2008). In this context that may be resulting from the fear of having an electronic health record of one's medical history. In our research context we also theorise that that Computer Anxiety to have a direct negative effect on the perceived attitude towards information control. As a result of these evidence and considerations the following hypotheses were formulated regarding Computer Anxiety represented in this context as Computer/EHR Anxiety.

Hypothesis 3: Computer/EHR Anxiety will have a direct positive effect on the consumers' perceived privacy concerns

Hypothesis 4: Computer/EHR Anxiety will have a direct negative effect on perceived acceptance of the technology

Hypothesis 5: Computer/EHR Anxiety will have a direct negative effect on information control

Similar to what has been seen in technology acceptance research in general, Computer Attitude is considered to have a significant effect on acceptance (Or & Karsh, 2009). Similar to anxiety, computer attitude can also influence privacy concerns with consumers. A similar hypothesis is also made in relation to information control. The following hypotheses are formulated regarding Computer Attitude represented in this context as Computer/EHR Attitude.

Hypothesis 6: Computer/EHR Attitude will have a direct negative effect on consumers' perceived privacy concerns

Hypothesis 7: Computer/EHR Attitude will have a direct positive effect on consumers' perceived acceptance of the technology

Hypothesis 8: Computer/EHR Attitude will have a direct positive effect on information control

Information privacy context

Information privacy related technology acceptance studies are mostly based on the big five personality traits (Graeff & Harmon, 2002; Korzaan & Boswell, 2008; Smith, Milberg, & Burke, 1996). But these studies were primarily focused on domains such as corporate use of personal information (Angst & Agarwal, 2009). Information privacy research in the healthcare domain, however, focuses on issues such as information sharing, information access and use, information control (Angst & Agarwal, 2009; Perera, Holbrook, Thabane, Foster, & Willison, 2011). Therefore in this study we adopt similar construct items to measure privacy concerns of individuals. This construct is important to the overall study of the thesis given our primary objective of addressing information privacy.

Privacy concerns are related to the consumer concern about information privacy arising from health information being stored and manipulated electronically (in the EHR system), information sharing by healthcare professionals and access and use of information by the said parties. As mentioned earlier, sharing and information access and use, have been directly associated with privacy concerns. Specific to this study, it was theorised that the privacy concerns would positively affect the consumers' perceived need of information accountability, the primary focus of this

thesis. Privacy concerns are also theorised here to have direct effects on the other two information context constructs because they are also directly related to IAF characteristics, which are addressed in chapters five and six. A direct negative effect on the perceived acceptance of the technology is also theorised. The resulting hypotheses are as follows.

Hypothesis 9: Privacy concerns will have a direct positive effect on consumers' perception of information governance

Hypothesis 10: Privacy concerns will have a direct positive effect on consumers' perception of information control

Hypothesis 11: Privacy concerns will have a direct positive effect on consumers' perception of information accountability

Hypothesis 12: Privacy concerns will have a direct negative effect on consumers' perceived acceptance of the technology

Trust, in this study, is related to the trust level of a consumer on a third party (Whiddett, et al., 2006b). Trust can affect both privacy concerns and the acceptance of technology. This construct related to the technological aspect, as discussed in chapter five, involving the health authority setting access policies for healthcare information. The characteristic was also identified as an eHealth requirement in section 1.2.6. It is important to understand how consumers perceive this characteristic of the IAF. It was also theorised that trust would have direct effect on all three information context constructs. Therefore the following hypotheses were made.

Hypothesis 13: Trust will have a direct negative effect on consumers' perceived privacy concerns

Hypothesis 14: Trust will have a direct negative effect on consumers' perception on information governance

Hypothesis 15: Trust will have a direct negative effect on consumers' perception on information control

Hypothesis 16: Trust will have a direct negative effect on consumers' perception on information accountability

Hypothesis 17: Trust will have a direct effect on consumers' perceived acceptance of the technology

Information context

The constructs of the information context are information control, information governance, and information accountability as discussed in chapter three, which directly relate to the characteristics of AeH systems and the technological aspects presented in chapters five and six. The results from chapter three showed that none of the three constructs had a direct relationship with behavioural intention. Rather than assuming the same here related to the consumers' perspective, because they have not been tested before elsewhere, it was theorised that all three constructs would have a positive direct effect on the acceptance of the technology. This is because consumers may perceive the three accountability measures could improve their information privacy as opposed to HCPs perceiving them as hindrances. The following three hypotheses were made to reflect these effects.

Hypothesis 18: Information governance will have a direct positive effect on consumers' perceived acceptance of the technology

Hypothesis 19: Information control will have a direct positive effect on consumers' perceived acceptance of the technology

Hypothesis 20: Information accountability will have a direct positive effect on consumers' perceived acceptance of the technology

Perceived acceptance

Perceive acceptance covers the same aspects as behavioural intention, which was discussed in chapter three. Therefore, it is theorised that the perceived acceptance of the technology will have a direct effect on the actual acceptance by the consumers. The actual acceptance of the designed EHR system cannot be tested as part of this research study. As mentioned in chapter three, the implementation of such a system is too complex for a single research study. However, once implemented, a longitudinal study may be carried out to test the actual acceptance of the system by both eHealth consumers and healthcare professionals. The following hypothesis was made in relation to the actual acceptance of the system by healthcare consumers.

Hypothesis 21: Perceived acceptance will have a direct positive effect on the actual acceptance of the IAF

The hypotheses are summarised in Table 4.1.

Moderators

In prior research relating to how consumers accept healthcare information technology, there is a lack of consideration of the effects of moderating variable towards acceptance (Or & Karsh, 2009). Therefore in this study, four moderating factors were considered; gender, age, computer literacy and the awareness of the PCEHR. The effects of these factors are discussed later in the chapter.

Table 4.1 Research hypotheses

Construct	Abbreviation	Hypothesis
Individual Context		
Computer self-efficacy	CSE	H1: Computer/EHR Self-Efficacy will have a direct positive effect on the consumers' perception on information control H2: Computer/EHR Self-Efficacy will have a direct effect on the consumers' perceived acceptance of the technology
Computer (EHR) anxiety	ANX	H3: Computer/EHR Anxiety will have a direct positive effect on the consumers' perceived privacy concerns H4: Computer/EHR Anxiety will have a direct negative effect on perceived acceptance of the technology H5: Computer/EHR Anxiety will have a direct negative effect on information control
Computer (EHR) attitude	ATT	H6: Computer/EHR Attitude will have a direct negative effect on consumers' perceived privacy concerns H7: Computer/EHR Attitude will have a direct positive effect on consumers' perceived acceptance of the technology H8: Computer/EHR attitude will have a direct positive effect on information control
Information Privacy Context		
Privacy Concerns	PC	H9: Privacy concerns will have a direct positive effect on consumers' perception of information governance H10: Privacy concerns will have a direct positive effect on consumers' perception of information control H11: Privacy concerns will have a direct positive effect on consumers' perception of information accountability

		H12: Privacy concerns will have a direct negative effect on consumers' perceived acceptance of the technology
Third party trust	TPT	H13: Trust will have a direct negative effect on consumers' perceived privacy concerns H14: Trust will have a direct negative effect on consumers' perception on information governance H15: Trust will have a direct negative effect on consumers' perception on information control H16: Trust will have a direct negative effect on consumers' perception on information accountability H17: Trust will have a direct negative effect on consumers' perceived acceptance of the technology
Information Context		
Information governance	IG	H18: Information governance will have a direct positive effect on consumers' perceived acceptance of the technology
Information control	IC	H19: Information control will have a direct positive effect on consumers' perceived acceptance of the technology
Information accountability	IA	H20: Information accountability will have a direct positive effect on consumers' perceived acceptance of the technology
Acceptance of the IAF		
Perceived acceptance	ACC	H21: Perceived acceptance will have a direct positive effect on the actual acceptance of the IAF

4.2.4 Survey items and constructs

The individual items used for measuring each of the constructs are given in Table 4.2. Although some items were adopted from previous research in technology acceptance, most of the items were specifically designed for this study. The reason for the low adoption from prior research was due to the nature of the respondents and the introduction of a new information manipulation protocol to EHRs.

Table 4.2 Constructs and questionnaire items

Construct	Related hypothesis	Questionnaire item	Origin
Individual Context			
Computer self-efficacy (CSE)	H1 H2	CSE1…. I would be able to complete different tasks without anyone around to tell me what to do CSE2…. I would be able to complete tasks if I could call someone for help if I got stuck CSE2…. I would like to have the guidance of a health authority in managing my health information electronically	Venkatesh et al., 2003 Developed for this research study
Computer/EHR anxiety (ANX)	H3 – H5	ANX1….I feel apprehensive about using this EHR systems ANX2….I would hesitate to use this EHR systems for fear of making a mistake I cannot correct ANX3….I would be concerned about losing a lot of information by hitting the wrong key ANX4….I would find this EHR systems intimidating	Venkatesh et al., 2003
Computer/EHR attitude (ATT)	H6 – H8	ATT1….I believe that paper records can be better utilised to keep health information more secure than in EHRs ATT2…. I think that using an EHR to manage my health information is a good idea ATT3….I think that EHR systems are expensive to implement and maintain. The expense could be better utilised to improve other healthcare facilities	Developed to capture eHR attitude Venkatesh et al., 2003 Developed to capture eHR attitude

Information privacy context			
Privacy concerns (PC)	H9 – H12	PC1…. I believe that storing and managing health information electronically (using computers) will threaten my privacy PC2….I feel that patient information, even with personal identifiable information removed, should not be accessed by any outside entity or authority (including the government) for any reason (including research) other than the caregiver(s) for the purpose of providing healthcare PC3…. I would prefer if health professionals who treat me had access to information that is **only related** to the current episode of care knowing that it would not hinder the healthcare process PC4…. I feel that caregivers should not be allowed to share patient information with other healthcare professionals PC5… I think that patient consent is critical before using patient information	Developed for this research study
Third party trust (TPT)	H13 – H17	TPT1…. I would trust a health authority to properly manage my health information so that my privacy requirements are satisfied TPT2…. I would trust a health professional such as my GP to properly manage my health information so that my privacy requirements are satisfied TPT3…. I believe that a health authority can formulate a comprehensive set of usage rules which would indicate what health data is required for treating a given medical condition	Developed for this research study

Information Context			
Information governance (IG)	H18	IG1…. I believe that when health information is manipulated electronically (using computers), health professionals should be bound by predefined rules for accessing and using patient health information IG2…. I believe that when health information is manipulated electronically (using computers), a comprehensive medical knowledge base should govern information usage IG3…. I believe that when health information is manipulated electronically (using computers), proper rules should be set on the use of health information IG4…. I would prefer to impose usage rules on health professionals who would access my health information for the purpose of providing healthcare knowing that those rules would not hinder the healthcare process	Developed to capture attitudes towards having usage rules and a computerised knowledgebase
Information control (IC)	H19	IC1….I believe that patients have the right to set their own privacy settings in an electronic health record system similar to that of most social media websites (e.g. Facebook) IC2…. I believe that patients have the right to decide which health professional can access his/her eHR IC3…. I would like to have control of my health information rather than trusting a health authority or a health professional with my data	Developed to capture attitudes towards patients participation and control of health information

Information accountability (IA)	H20	IA1…. I believe that if usage rules set by a health authority are broken intentionally, the offenders (e.g. doctors, nurses, etc) should be held accountable IA2…. I think that patients have the right to inquire about possible misuse of their health information IA3…. I think that health professionals should be required to justify why they have accessed/used information which they did not require for a given episode of care IA4…. I feel that health professionals should be held accountable if they fail to provide a valid justification for a patients' inquiry IA4…. I feel that health professionals should be held accountable if found to have misused patient health information. (Misuse in this context is using information for tasks other than the purpose of patient care which would have a negative impact on the patient's social life, professional career, etc)	Developed to capture the attitudes towards accountability measures
Acceptance of the technology			
Perceived acceptance	H21	ACC1…. I would use this type of EHR system to manage my health information in the future ACC2…. I am confident that my privacy will be secure in this type of EHR system ACC3…. I feel that using this type of EHR system would hinder my well-being	Developed for this research study

4.3 PARTICIPANTS

4.3.1 Selection criteria

The participants were selected from the Science and Engineering Faculty at the Queensland University of Technology, Brisbane, Australia. All participants were students studying in non-health related undergraduate and postgraduate courses. This was to eliminate the influence of possible bias towards the questionnaire items affecting from the healthcare knowledge and the study environment of those students. Since the students from the health related courses participated in the study reported in chapter three, they were not engaged in this study. Apart from the reasons mentioned above, the selection of this specific population also depended on the willingness of the institution to broadcast the survey invitation emails within the institution.

4.3.2 Participants

The participants comprised of undergraduate and postgraduate students studying non-health related courses at the institute. The distribution is shown in Table 4.3.

Table 4.3 Distribution of respondents

	Undergraduate		**Postgraduate**		
	Male (%)	***Female (%)***	***Male (%)***	***Female (%)***	**Total**
1st Year	28 (32.6)	18 (36.7)	13 (52.0)	12 (46.2)	71
2nd Year	26 (30.2)	10 (20.4)	5 (20.0)	5 (19.2)	46
3rd Year	16 (18.6)	14 (28.6)	5 (20.0)	2 (7.7)	37
4thYear	15 (17.4)	6 (12.2)	1 (4.0)	2 (7.7)	24
Graduated	1 (1.2)	1 (2.0)	1 (4.0)	5 (19.2)	8
	86	**49**	**25**	**26**	**186**
	135		**51**		

The age of the respondents ranged from a minimum of 17 to a maximum of 65 with a mean of 27 (SD = 10.1.). Table 6.4 shows the age distribution.

Table 4.4 Age range of respondents

Age Range	Number of Respondents
17 - 20	58
21 - 30	77
31 - 40	26
41 - 65	23
Total	**184**
Note: Age had two missing values	

4.4 THE SURVEY

4.4.1 Instrument

Similar to the questionnaire used in chapter three, the questions were included in an online survey tool and were formatted such that the readability and presentation of the survey was appropriate. Questions were distributed in such a way that the ceiling and floor effects were minimal. The survey was distributed via email invitation to all prospective participants (see Appendix B the for email invitation). Because all university students were already familiar with email and Internet technologies, there were no hindrances expected from the use of an online survey tool in terms of usability. The online survey distribution and response collection was also expected to maximise the response rate.

4.4.2 Survey Administration

A detailed description was given to the participants outlining the specific characteristics of the EHR system. Similar to chapter three, the survey questions were designed to further outline the characteristics specific to the IAF such as policy setting by patients and inquiries and justifications. The questions focused on the attitudes the respondents had on an EHR system designed using the IA principles. A screen shot of the first page of phase 1 survey can be found in Appendix C, which is similar to phase two. After six weeks time from the launch of the survey, data collection was terminated.

4.4.3 Ethics and Limitations

Ethical clearance was obtained from Queensland University of Technology to conduct the research study as a variation of the ethics clearance obtained for the

study presented in the previous chapter, which also did not include any health and safety issues. The ethical clearance certificates can be found in Appendix A.

As previously stated, the study was limited to a student population. Initial attempts were made to involve members of the general public in the survey and were unsuccessful. The decision was made afterwards to include a suitable student cohort that would deliver a limited but similar result to what could have been expected from current healthcare professionals. This was done so that the research study could be completed within the available time frame.

4.5 DESCRIPTIVE ANALYSIS OF THE RESULTS

The descriptive analysis presented in this section aim to find the overall attitude towards the designed IAF for eHealth systems. The results from the descriptive analysis also aids to establish the practical significance of the research questions (Hair, et al., 1998).

4.5.1 Response

A total of 259 responses were received. But due to incomplete submissions, 73 were removed from the analysis. The descriptive results reported here are from the resulting 186 responses. Limited amount of quantitative data were also collected in the form of unrestricted comments.

4.5.2 Analysis

A total of 33 items were used to measure the 9 model variables, which are used to assess the measurement model, structural model and hypotheses. An additional 7 questions were also included in the questionnaire relating to the EHR system. The response for the model variables is summarised in Table 4.5.

Table 4.5 Descriptive data of questionnaire items related to the measurement model

	Strongly Disagree		%		Strongly Agree		
	1	**2**	**3**	**4**	**5**	**Mean**	**SD**
Computer/EHR Self-Efficacy						**3.96**	**.850**
CSE1	.5	6.5	14.5	46.2	32.3	4.03	.882
CSE2	1.6	3.2	12.4	51.1	31.7	4.08	.844
CSE3	1.6	5.4	23.1	55.4	14.5	3.76	.826
Computer/EHR Anxiety						**2.40**	**1.121**
ANX1	14.5	38.2	21.0	22.0	4.3	2.63	1.108
ANX2	17.7	43.5	12.4	21.5	4.8	2.52	1.154
ANX3	25.3	43.5	12.9	14.0	4.3	2.28	1.120
ANX4	30.1	41.4	12.9	11.8	3.8	2.18	1.103
Computer/EHR Attitude						**3.52**	**1.124**
ATT1*	7.5	14.5	22	31.7	24.2	3.51	1.218
ATT2	2.7	5.4	22.6	41.9	27.4	3.86	0.971
ATT3*	12.9	12.4	25.8	38.7	10.2	3.21	1.183
Privacy concerns						**3.3**	**1.208**
PC1	11.8	32.8	21.0	25.3	9.1	2.87	1.188
PC2	9.7	25.3	11.8	24.2	29.0	3.38	1.383
PC3	13.4	23.7	15.1	37.1	10.8	3.08	1.256
PC4*	8.6	24.7	22.6	34.4	9.7	3.12	1.147
PC5	1.6	13.4	3.8	40.3	40.9	4.05	1.064
Third Part Trust						**3.78**	**.978**
TPT1	3.8	10.8	12.9	53.2	19.4	3.74	1.014
TPT2	1.6	9.7	14.0	51.1	23.7	3.85	.945
TPT3	2.2	11.8	15.1	51.6	19.4	3.74	.974
Information Governance						**4.20**	**.820**
IG1	1.1	1.1	5.9	40.9	51.1	4.40	.745
IG2	1.1	5.4	18.8	46.2	28.5	3.96	.887
IG3	.0	1.1	3.8	40.3	54.8	4.49	.626
IG4	2.2	10.2	10.8	43.5	33.3	3.96	1.023
Information Control						**3.65**	**1.130**
IC1	4.8	15.6	12.4	36.6	30.6	3.73	1.192
IC2	1.6	13.4	9.7	43.0	32.3	3.91	1.049
IC3	2.7	28.0	22.6	28.0	18.8	3.32	1.150
Information accountability						**4.46**	**.720**
IA1	.5	2.7	4.3	33.3	59.1	4.48	.751
IA2	.0	.0	2.7	33.9	63.4	4.61	.542
IA3	2.7	2.2	5.9	38.7	50.5	4.32	.890
IA4	0	3.8	7.5	37.6	51.1	4.36	.781
IA5	.0	.5	5.9	33.3	60.2	4.53	.634
Perceived acceptance						**3.67**	**.931**
ACC1	1.6	5.4	30.1	40.9	22.0	3.76	.911
ACC2	5.9	12.9	33.3	38.2	9.7	3.33	1.016
ACC3*	1.1	4.3	22.0	46.2	26.3	3.92	.867
Note: * reverse coded item							

Computer/EHR self-efficacy

An overall mean of 3.96 (0.850) was achieved for CSE. All items used to as measures exhibited means significantly greater than the midpoint of the scale. This indicates that the respondents were confident about their ability to use the EHR system and their computer skills are high. This was expected since the respondent cohort was from a technology oriented faculty at the Queensland University of Technology.

Computer/EHR anxiety

The overall mean for ANX was 2.40 (1.121) with all items used as measures having means less than the midpoint of the scale. The respondents exhibited a low level of anxiety in using the EHR system to manage their health information but the level was not very low. This significant level of anxiety may contribute to increase of privacy concerns and may negatively affect acceptance, which will be tested later in the study.

Computer/EHR attitude

The respondents' computer/EHR attitude is high with the means of all measurement items above the midpoint and an overall mean of 3.52 (1.124). But the level is not very high.

Privacy concerns

The overall mean of the measurement items for PC was 3.3 (1.208). This indicates that the respondents did have considerable privacy concerns but it was not strong. This may be due to the age group of the participants, who have not had extensive exposure to a medical system and had to manage their sensitive health information.

Third party trust

The respondents exhibit a relatively high level of trust on health authorities and their caring physicians towards the management of their health information. The overall mean for TPT was 3.78 (0.978).

Information governance

The respondents strongly believe that information governance measure such as usage rules and computerised medical knowledge bases are required in the system. The overall mean for IG was a significantly high 4.20 (0.820). This high indication is a favourable sign for the application of information accountability in eHealth.

Information control

The respondents believe that general consumers must be allowed to control their own information. The overall mean of IC was a moderately high 3.65 (1.130). Since information control is a key characteristic of AeH system, it was expected that this level would be higher than exhibited. IC3 has had a significant contribution to the mean level. This reflects the high third party trust level exhibited by the respondents.

Information accountability

The overall mean score for IA was a very high 4.46 (0.720). This indicates that the respondents very strongly believe that information misuse must be followed by appropriate accountability measures. The respondents' attitudes towards the inquiry and justification process are very favourable. This indicated that the respondents are very keen on this capability, a favourable sign for AeH systems.

Perceived acceptance

The overall mean score for ACC was 3.67 (0.931). The mean scores for all items used to measure the construct was above the midpoint of the scale. But the levels are not very high as exhibited for some of the other constructs. Nevertheless, the current perceived acceptance levels are favourable.

Overall response

The mean score for each model variable were higher than the midpoint of the scale except for Computer/EHR Anxiety. This indicates the strength of the respondents' agreements with the items used to measure each of the constructs. The mode of each of the items used to measure the constructs, except Computer/EHR Anxiety, was 4. This is an indicator that the majority if the respondents were not neutral in their response but were in agreement with the items.

4.5.3 Qualitative Analysis

The qualitative data was obtained from the questionnaire through unrestricted comments. The respondents commented on their attitudes towards managing their health information on the designed EHR system and the importance of the accountability features presented. A total of 56 respondents commented on the EHR system. The comments are categorised in to themes and presented in Table E.1 of Appendix E.

There is a strong bias towards consumers' right to control their healthcare information as a means of privacy management. As one respondent said;

"The term 'Sufficient reasoning' should be up to the end user, through privacy settings NOT Government Legislators"

This indicates that patients should have the right to inquire about any potential misuse of their information and that it is their right to do so. It was also seen important to clearly identify the type of use that might occur outside of the set rules.

"If they are misused in some insidious plot to cause harm or I dunno spread my info across the Internet yeah sure. But if their intent is too better treat a patient or use the data in some reasonable medical way(such as research), only they happen to break some small rule in information usage, meant only to ensure a patients impression of privacy while limiting practical use of data, then no, they shouldn't be punished, instead the rules should be adapted to the needs of the health professionals."

"If they are found to have misused the information then that should be the same as breaking patient confidentiality. If they have used it for researching patients with conditions similar to one of their own, or to help the patient then I do not think it is a bad thing."

The validation of the justifications must consider the circumstances which the usage occurred. The patients' health must come first.

As one respondent commented saying, "*Misuse should be made a criminal offence to discourage it*", a strong statement but this indicates that accountability measures can deliver the deterrence required to prevent users from misusing information. Other similar comments were present that exhibited the need and the effectiveness of accountability measures in the EHR system.

There were negative comments directed towards both EHRs in general, where one respondent commented saying; *"Don't waste money on eHR"*, and the designed EHR system with IA. However, the majority of the comments from the respondents towards the designed EHR system were positive; one respondent saying that it was a "*Great idea*".

General consensus was that the idea was appropriate for the management of healthcare information electronically. Although the response was favourable to the proposed EHR, more extensive work need to be done, especially with a broader age range and a more general cohort, to further validate the consumers' attitudes towards information accountability in eHealth.

4.6 ASSESSMENT OF THE RESEARCH MODEL AND HYPOTHESIS TESTING

For the assessment of the research model and hypothesis testing, the same methods used in the previous chapter are used here. The partial least square (PLS) method is used to assess the research model. As mentioned before, this involves the assessment of the measurement model and the assessment of the structural model (hypothesis testing).

4.6.1 Assessment of the measurement model

Construct reliability and discriminant and convergent validity of PLS analysis were used to measure the reliability and validity of the measurement model respectively.

Construct reliability

Construct reliability of the measurement model was determined by the individual item loadings, internal consistency and the average of variance extracted (AVE). Tables E.2 and E.3 in Appendix E present the results in the order above. The PLS results indicated that all construct measurements were reliable since the individual item loadings were greater than the 0.3 threshold (Igbaria, et al., 1997). Therefore, all items were used for the proceeding analysis. The composite reliability of the constructs revealed that all reliabilities were greater than the 0.707 threshold required (Igbaria, et al., 1997). The average variance extracted (AVE) for each construct showed that they were greater than the required 0.5.

Discriminant and convergent validity

The construct validity was determined by measuring the discriminant and convergent validity. Discriminant validity is used to measure the difference of a construct to other constructs used in the model (Schaper, 2009). Convergent validity is used to determine the convergence of the items used to measure a construct. It shows how they associate with each other to reflect the construct they are designed to measure (Datmar Straub, et al., 2004). In PLS, correlations of the constructs and cross loading of constructs are used to determine the discriminant and convergence validity.

Correlation of constructs

In the measurement of correlation of constructs, the square root of AVE must be greater than the correlation with other constructs (Datmar Straub, et al., 2004). Table E.4 in Appendix E shows the correlation of constructs with the square root of AVE (shown in bold). None of the items had a higher value than the square root of the corresponding AVE. Overall, discriminant and convergent validity is acceptable.

Cross loadings of constructs

Cross loadings of constructs reveal the fit of individual items load on the latent variable compared to their loadings on other variables (Schaper, 2009). The cross loadings are shown in Table F.5. The cross loadings of the constructs revealed that the loadings for each of the indicators are significantly higher than those of the other constructs. We come to the conclusion that the discriminant validity of the model indicators is acceptable because the indicators used reflect the constructs they are supposed to than other constructs.

4.6.2 Assessment of the structural model

Assessment of the structural model reveals the significance of the hypotheses in the model. The process involves testing the predictive power of the model and the significance of the relationships between the models' constructs (Schaper, 2009).

Predictive properties of the model

The predictive power of the model was established by performing PLS analysis. R^2 values of the entire model were produced and for each of the dependent variables. The results are shown in Table 4.6.

Table 4.6 Predictive properties of the model

Construct	R^2 Value
Privacy Concerns (PC)	0.361
Information Governance (IG)	0.194
Information Control (IC)	0.386
Information accountability (IA)	0.089
Perceived acceptance (ACC)	**0.698**

The results revealed that the model was capable to explain 69.8% of the perceived acceptance of the participants of the IAF. This predictive power of the model is a highly satisfactory level in technology acceptance research. The model was also able to predict 36.1% of variance in privacy concerns, 38.6% of variance of information control, 19.4% of variance of information governance and 8.9% of variance of information accountability.

Relationship between model constructs

To establish the relationship of the model constructs, the path coefficients and t-values for each of the structural model paths were calculated. Seventeen of the 18 hypotheses are tested here. From the available technology acceptance literature we assume a direct relationship between BI and actual use behaviour contributing to the acceptance of the IAF.

A bootstrapping resampling technique was used to calculate the values using smartPLS. The analysis used 100 randomly selected samples from the 186 cases. The corresponding p-values were determined using an F-distribution table and the values used were given in Table 3.14. The results of the bootstrapping and PLS analysis are summarised in Figure 4.2 and Table 4.7.

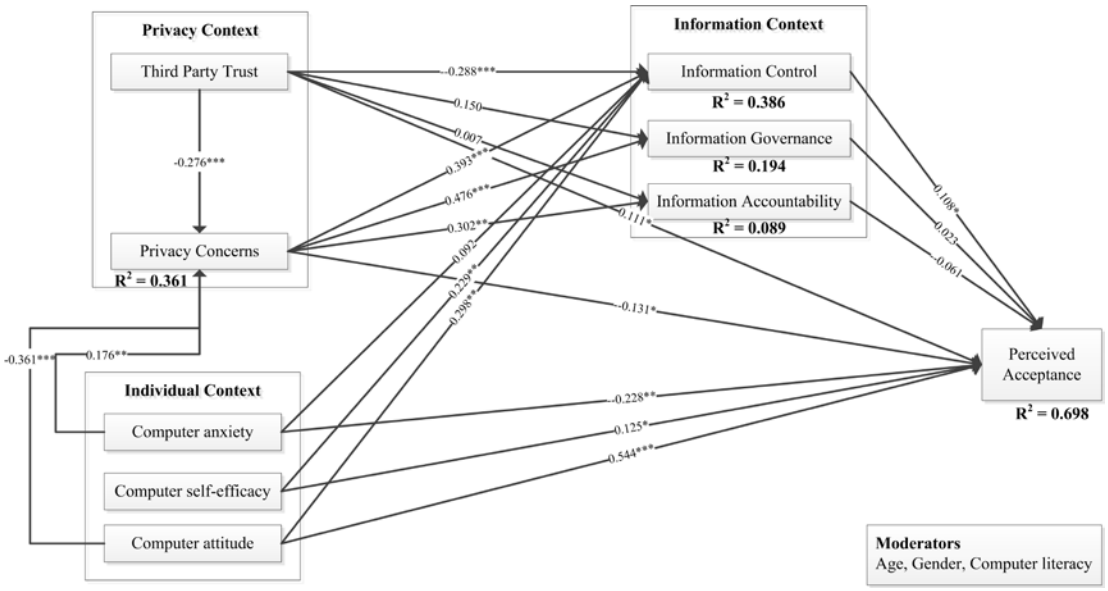


Figure 4.2 Results of the structural model

The research model revealed that only the individual context constructs has a significant effect on the perceived acceptance of the technology.

Table 4.7 Individual path significance

Path	t-Statistics	Path Coefficient	Hypothesis
CSE → IC	3.299**	0.229**	H1
CSE →ACC	2.268*	0.125*	H2
ANX →PC	2.601**	0.176**	H3
ANX →ACC	3.339**	-0.228**	H4
ANX →IC	1.149	0.092	H5
ATT → PC	4.919***	-0.361***	H6
ATT →ACC	9.595***	0.544***	H7
ATT →IC	3.421**	0.298**	H8
PC →IG	4.566***	0.476***	H9
PC →IC	4.959***	0.393***	H10
PC →IA	3.863**	0.302**	H11
PC →ACC	1.972*	-0.131*	H12
TPT →PC	4.189***	-0.276***	H13
TPT →IG	1.065	0.150	H14
TPT →IC	4.133***	-0.288***	H15
TPT →IA	0.076	0.007	H16
TPT →ACC	2.299*	0.111*	H17
IG →ACC	0.532	0.023	H18
IC →ACC	2.020*	0.108*	H19
IA →ACC	1.305	-0.061	H20

The results of the hypothesis testing revealed that five (H5, H14, H16, H18 and H20) of the twenty tested hypotheses were not supported by the results. Privacy concerns (PC) exhibited a significant negative effect of the perceived acceptance. This indicates that if an eHealth consumer felt concerned about their privacy in the systems, they are less likely to adopt the system, thus confirming our thesis that information privacy concerns of consumers are a significant aspect for eHealth systems. The results revealed that there was no positive or negative effect from the information context towards the perceived acceptance except IC, which had a positive significant effect. Privacy concerns had significant positive effects on IG, IC and IA, supporting our hypotheses H9 – H11. This indicates that if an eHealth consumer is concerned about privacy, they believe that the measures put in place by the IAF are required, thus required aspects for an EHR system, which is favourable to the rest of the study. Trust also plays a significant role in the research model presented. The level of trust the respondents had on third parties had a significant negative effect on PC and IC, thus supporting our hypotheses H13 and H15 respectively. This indicates that privacy concerns are high when the trust levels are low and that the respondents believed that they should have the control of their own health information. Therefore, by providing the consumers the control of their information, the IAF caters for a need that would improve system acceptance, which is supported by the evidence relating to H19 where IC shows a significant contribution to system acceptance. By not providing evidence for H18 and H20, IG and IA showed no significant effects on overall system acceptance. However, as discussed above, given their significant relationships with PC, the information context constructs, the information accountability characteristics are significant EHR system requirements for better privacy management. We believe that when consumers are exposed to an EHR system that is similar to the one proposed, IA and IG may show positively contributing effects to overall system acceptance.

The constructs measured in relation to the individual context also show significant effects on PC, IC and ACC. Computer/EHR anxiety shows a significant positive relationship with PC and a significant negative relationship with ACC, which is indicated by the supporting evidence for H3 and H4 respectively. Therefore, if an eHealth consumer's anxiety levels are high their privacy concerns will be high and they are less likely to accept the EHR system. Because our descriptive analysis

in section 4.5 showed a low anxiety level, we can assume that the proposed EHR system with the IAF is likely to be adopted by future eHealth consumers. However, we note that the anxiety level was not as low as expected, a results we believe is due to the fact that the concept of information accountability is new to the respondents. Given the necessary exposure however, we believe that the anxiety levels would decrease to a more favourable level. Similar arguments can be made in relation to Computer/EHR attitude, reflected through H6 and H7. Although by not supporting H5, ANX did not have a significant effect on IC. But ATT showed a significant positive effect on IC, supporting H8. As indicated from a supported H1, computer/EHR self-efficacy also positively affects IC.

Total effects on perceived acceptance

As argued in chapter three, the total effect of each of the constructs on (in this case) the perceived acceptance of the respondents is another deciding factor that reveals the indirect effects. Using the same method as before, the total effects of each construct on perceived acceptance can be calculated. Table 4.8 show the results of the calculations.

Table 4.8 Total effects on perceived acceptance

Construct	Total effect
Computer self efficacy	0.1443**
Computer/EHR anxiety	-0.2332**
Computer/EHR attitude	0.6049***
Privacy Concerns	-0.089
Third Party Trust	0.1043*
Information governance	0.0233
Information control	0.1081*
Information Accountability	-0.0602

Computer/EHR Attitude has the largest total effect on perceived acceptance. Computer/EHR Anxiety also has a high negative effect on perceived acceptance. Privacy concerns have very low effect on perceived acceptance and the effect is not significant. Third party trust has a significant positive effect on perceived acceptance. Only information control from the information context constructs have a significant effect on respondents' perceived acceptance of the EHR system, which is positive.

4.6.3 Influence of the moderating variables

As previously stated, there is a lack of consideration of the effects of moderating variable towards acceptance in prior research relating to how consumers accept healthcare information technology (Or & Karsh, 2009). To test the effects of moderating variables, age, gender and computer literacy and the awareness of the PCEHR system have been considered here in this study. Table 4.9 shows the distribution of the data set in the moderating categories.

Table 4.9 Moderating variable categories

Moderating variable	Category	Number of cases (%)
Gender	Male	111 (59.7)
	Female	75 (40.3)
Age (years)*	17 – 21	71 (38.6)
	22 – 31	70 (38.0)
	32 – 65	43 (23.4)
Computer literacy	Excellent	137 (73.7)
	Good	43 (23.1)
	Moderate	6 (3.2)
Knowledge of the PCEHR	Aware	136 (73.2)
	Not aware	50 (26.8)
Note: * Age had two missing values		

Separate data sets for the different groups were created using SPSS Version 19. The following tables summarise the results of the PLS and bootstrapping analysis performed on each category. The results for each moderating variable and their categories are shown in Tables 6.15 to 6.18. The hypotheses shown in red in each table are the unsupported hypotheses from the original results.

Gender

A total of 111 male respondents and 75 female respondents were present in the 186 responses. The PLS and bootstrapping results for male and female respondents are shown in Table E.6 of Appendix E. Although none of the rejected hypotheses were supported by either of the groups, the difference in male and female responses is significant. Notably, privacy concerns and computer-self efficacy did not exhibit significant relationships to acceptance in either group. Females were not sensitive to

most of the hypothesised relationships as males. Therefore, gender can be seen as a moderating variable in this study.

Age

The data set was divided into three main age groups: 17 – 21 (n = 71), 22 – 31 (n = 70) and 32- 65 (n = 43). The analysis results for each of the groups are shown in Table E.7 of Appendix E. The deviation from the original results increased with age. The originally unsupported hypotheses remained unsupported with all three groups. Privacy concerns did not exhibit a significant relationship to the acceptance in any of the groups and neither did computer self efficacy, third party trust and information control as was seen in the original results.

Computer Literacy

Computer literacy was categorised into two main groups due to the fact that only 6 respondents indicate a moderate computer literacy and none of the respondents indicated otherwise. Those six responses were removed from the analysis. The two groups were populated such that 137 respondents were included to the *Excellent* group and 43 respondents to the *Good* group. The results of the analysis are shown in Table E.8 of Appendix E. The results deviated from the original results in the group with *Good* computer literacy (note that the number of respondents were less than the required 60 for reliable PLS analysis). Privacy concerns, computer self-efficacy and information control did not exhibit a significant relationship with acceptance in either group as seen from the original results. Similar to chapter three, general conclusions cannot be drawn as regards to the moderating effects of computer literacy.

Awareness of the PCEHR

The awareness of the PCEHR was categorised into two groups: Aware (n = 136) and Not Aware (n = 50). The PLS and bootstrapping results are show in Table E.9 of Appendix E. The results of the group of respondents who did not know about the PCEHR exhibited no significant relationships. But the number of respondents were less than the required 60 for reliable PLS analysis. Notably, the respondents who were aware of the PCEHR exhibit a significant relationship between information accountability and acceptance.

From the results presented above, it is seen that all moderating variables do affect the research model. However, the interactions amongst the moderating variables were not tested in this study. But such a study is encouraged to understand the full effect of the moderating factors on the models' relationships.

4.7 DISCUSSION AND CONCLUSION

In this chapter, we have presented the results of a survey conducted to measure the attitudes of general EHR consumers towards an EHR system with information accountability measures for information privacy management. We presented a descriptive analysis of the results and validated an empirical research model that can be used to measure the effects of each of the characteristics of the model towards the consumers' perceived acceptance.

The results of the descriptive analysis of the quantitative and qualitative results showed that such a system would be favourably received by general consumers. The respondents indicated that they favour the newly introduced information accountability measures (conclusions drawn from the results relating to the information context constructs). Previously well established survey items from related research studies performed as documented elsewhere indicating that the survey cohort behaved similar to more general populations although they were students. A limitation of selecting university students is a possible presence of bias from well educated respondents. All eHealth consumers are not so.

Although the information context constructs did not have significant positive effect on perceived acceptance, other constructs like privacy concerns had significantly high effects on them. This indicates that the need for those measures is high in the minds of the consumers and the relationships indicate that with high privacy concerns, the need for those measures increase. Only information control positively affects system acceptance. Information Governance and Information Accountability did not exhibit a significant positive or negative effect. This is a acceptable outcome for the rest of the study.

From the results obtained, we can also conclude that personal beliefs relating to one's ability to use and attitudes about computing has the most effect on the acceptance of technology.

Previous research has shown that, patients who have experience with EHR through their caring doctor (e.g. GP) exhibit significant relationships between their privacy concerns and their acceptance of medical technology (Jessica S. Ancker, Edwards, Miller, & Kaushal, 2012). But more recently, studies have found that experience with physicians using EHRs was not associated with privacy (Jessica S Ancker, Silver, Miller, & Kaushal, 2012; Whiddett, et al., 2006b). Therefore, further analysis is required to determine the effect of privacy concerns towards the acceptance of EHR systems adoption by consumers in general, which will not be addressed in this thesis.

The effects of several moderating variables were also tested. The originally rejected hypotheses remained invalid with all moderating variable results except for the awareness of the PCEHR, which indicated a significant negative relationship of information accountability and acceptance with the respondents who were aware of the PCEHR. This negative effect could be due to indirect effects of privacy concerns on the information accountability construct. Further work is required to find conclusive evidence for this effect.

The results showed that there is a negative relationship between trust and privacy concerns. Therefore, if trust levels are low, the privacy concerns will be high and vice versa. Trust also had a negative relationship with information control, which indicates that low levels of trust will result in a high need for personal control of information.

To improve clarity and connectivity of the thesis, the outcomes of this chapter can be related to the case scenario similar to what was discussed in chapter three. However, the perceptions towards each construct in this chapter are different from what was observed in chapter three given that they measured the consumers' perspective as opposed to the professionals' perspectives in chapter three. In our case scenario, the survey results focus on Patient X's perspectives on the EHR system in question. Patient X is capable of selecting the HCPs he/she prefers to have access to his/her EHR and define custom access policies for them. This fact is captured through the construct IC. From the survey results, we saw that IC is positively related to ACC, thus supporting our hypothesis H19. If Patient X believes that his computer/EHR self-efficacy is high and his attitude towards EHRs is positive, he would strongly believe that having control of his EHR information is appropriate.

These facts are supported by hypotheses H1 and H8 respectively. Patient X's information privacy concerns also play a significant role in relation to the information context constructs, which are directly related to the IAF characteristics. If Patient X's privacy concerns are high, he strongly believes that the three IAF characteristics IG, IC and IA are suitable for implementation in EHR systems. As discussed earlier, this fact is indicated from the strong evidence for H9, H10 and H11.

We conclude that information accountability measures are important to the management of information privacy in eHealth systems that utilise EHRs. EHR consumers are favourable towards the introduction of these measures in to eHealth systems and will adopt such systems if they are implemented in the near future. Further studies that test the effects of information accountability measures can be performed and is encouraged with the use of the presented research model.

Part Two: Technical Aspects

Chapter 5: Access Control Requirements for Accountable-eHealth Systems

In this chapter, we present access control requirement for AeH systems. We present and validate an access control model towards the design of a technical architecture of AeH systems. The model is designed by capturing distinctive features of well established access control models. The purpose, therefore, of this new access control model is to capture the requirements of eHealth stakeholders into one module that can be adopted in a working EHR system that facilitate accountability principles as presented in chapter two. Research objective 3(a) is addressed in this chapter.

5.1 INTRODUCTION

Information security encompasses three main characteristics; confidentiality, integrity and availability (Bishop, 2004; Gollman, 2009). Confidentiality deals with limiting access to information to only the authorised entities whilst integrity and availability deals with the prevention of unauthorised modification of information and the prevention of unauthorised withholding of information respectively.

Security measures of electronic health records (EHR) are a critical aspect of eHealth solutions, which use EHRs as the health information repository. Various solutions have been proposed and developed over the years but the questions still remains as to whether the data in EHRs are secure enough. Securing the storage and transmission of data alone is insufficient for the confidentiality of EHRs to be protected.

Access control is a fundamental security measure to assure that the information is accessed by the appropriate users. Therefore, access control deals with data access of authenticated users. Authentication is the initial stage of validation of the users to determine whether they are who they claim they are (Sandhu, Coyne, Feinstein, & Youman, 1996). Once authenticated, the users can enter an information system but access to information will still be governed by an access control policy that is contextual to the application domain. Access control models hence assume that users are authenticated to access the information system thus aims to control the data

access of such users (Sandhu & Samarati, 1994) and is one of the main safeguards against improper data access. The access control mechanism will determine what information each user is authorised or not authorised to access.

Many different access control models have been proposed. Amongst them, discretionary access control (DAC) (Sandhu & Samarati, 1994), mandatory access control (MAC) (Ferraiolo, Kuhn, & Chandramouli, 2003; Lindqvist, 2006; Osborn, 1997) and role based access control (RBAC) (Sandhu, et al., 1996) can be seen as well established models. The access control model presented here draws from the principles of these models and contextualises the principles to fulfil and balance the requirements of each type of consumers of an eHealth system. Focus is also given to purpose based access control (PBAC) (J. W. Byun, E. Bertino, & N. Li, 2005; Naikuo, Howard, & Ning, 2007) to fulfil the need to capture the purposes for data access by users.

Access control is a vital part of eHealth systems and proper access control policies are a necessity for any eHealth systems' operation (Motta & Furuie, 2003; National E-Health Transition Authority, 2011a). The nature of the domain makes its data access requirements different from other domains. Healthcare providers have information access requirements to fulfil their professional responsibilities and patients have information privacy requirements, which is a right they can exercise to not have their private information unnecessarily exposed resulting from the lack of confidentiality measures within a system. These requirements may in some instances, contradict each other and fulfilling every such requirement is a complex yet necessary task in order to implement apposite eHealth systems and also to gain the confidence and trust of the end users towards such systems.

5.2 RELATED WORK

In this section we will discuss the aforementioned access control models and access control approaches in eHealth. The access control models reviewed in this section have gone through many alterations and extensions within computer science research. However, the fundamental principles behind each model still remain core within most applications.

5.2.1 Access control in healthcare

Healthcare information systems contain sensitive information that is vital for healthcare providers to make crucial decisions regarding a patients' health. Information cannot always be denied to the treating healthcare professional due to underlying access policies. This means that traditional access control models are not suitable for a domain such as healthcare. To this end, many specialised access control models have been designed to address specific healthcare needs. It has been observed that access control research in the healthcare domain reflects the pace of generic access control research (Ferreira, Cruz-Correia, Antunes, & Chadwick, 2007), but they have their own limitations (Røstad, 2008).

The main focus on security threats of EHRs are related to data breaches to external entities (Burdon, Lane, & von Nessen, 2010; Demuynck & De Decker, 2005; Kierkegaard, 2012). Techniques such as cryptography address issues in relation to data security relating to external entities but internal data security issues such as who has access to what information cannot be addressed using such technologies. In fact, data breaches in relation to EHRs are also related to internal breaches (Kierkegaard, 2012). To this end, access control techniques are applied to EHRs, which can control the internal activities in relation to data access.

Different access control strategies for eHealth systems have also been developed in the past (Alhaqbani & Fidge, 2008; Motta & Furuie, 2003). Alhaqbani et al. (2008) showed that neither MAC, DAC nor RBAC could satisfy specific healthcare requirements they have previously identified but a careful combination of the models can address them successfully. In their model, patients can set sensitivity labels on data items and so can the caring medical practitioner to hide certain information from the patient in special circumstances. The patients' policy will act as a rigid access control for healthcare professionals unless the episode of care is declared as an emergency. But in a specialised domain such as healthcare, this rigid access control set by the patient is not suitable given that the patient is not always aware of complex medical relationships present between healthcare data types. Therefore, access policy formulation process must be overlooked by a healthcare authority that would make sure that the required information is always available to the relevant healthcare professional.

The most common access control model used in healthcare information systems is RBAC (Ferreira, et al., 2007; Røstad, 2008). The reason for this preference is due to its easier administration and flexibility to be adapted to the workflows and hierarchical needs of an organisation (Ferreira, et al., 2007).

One of the main aspects of privacy preservation in relation to information manipulation is the intended purpose of data collection (J. W. Byun, et al., 2005; Jin, Ahn, Covington, & Zhang, 2008; Jin, Ahn, Hu, Covington, & Zhang, 2009). It is widely regarded that data must be used for the purpose for which they have been collected. In this regards, purpose based access control (PBAC) models have been proposed for use in the healthcare domain (L. Sun, Wang, Soar, & Rong, 2012; Yang, Barringer, & Zhang, 2007). More general models using the PBAC approach are also presented that can be utilised in healthcare (J.-W. Byun, E. Bertino, & N. Li, 2005). An access control model in an EHR system therefore must be capable of identifying the intended purposes of a data element and also the access purpose of a user. It also follows that the data elements must be individually identifiable as seen in the eHealth requirements in section 1.2.6. Thus, a purpose based access control component must be integrated into the access control model. The definition of the purposes must be handled with care to avoid wrongful denial of information to healthcare professionals for legitimate access requests.

5.2.2 Prominent access control models

Discretionary access control

Discretionary Access Control uses access restrictions set by the owner of the data object to restrict access to the objects. The users are bound by the authorisations which specify the operations each user can perform on specified objects such as read (R), write (W) and execute (EXE) (Sandhu & Samarati, 1994). The DAC model uses an access control matrix to assign access rights to users. A simple access control matrix is shown in Table 5.1.

Table 5.1 Access control matrix

User	*Object 1*	*Object 2*	*Object 3*	*Object 4*
Dr. P	R,W, EXE	R,W	-	R,W, EXE
Dr. S	R,W	-	R,W, EXE	-
Dr. B	-	R,W, EXE	R, W	-
Dr. M	-	-	-	R,W, EXE

Implementing this matrix in large systems is a tedious and error-prone task and representing it as a matrix will consume a considerable amount of resources. To represent it in a practical system the most common approach is by means of an Access Control List (ACL) and a Capability List (CL). An ACL is used to associate each object, e.g. EHR data element, with the users who can access it. This association also contains the type of access (R, W, and EXE) to the object. This is a column wise representation of the access matrix. Figure 5.1 shows an ACL.

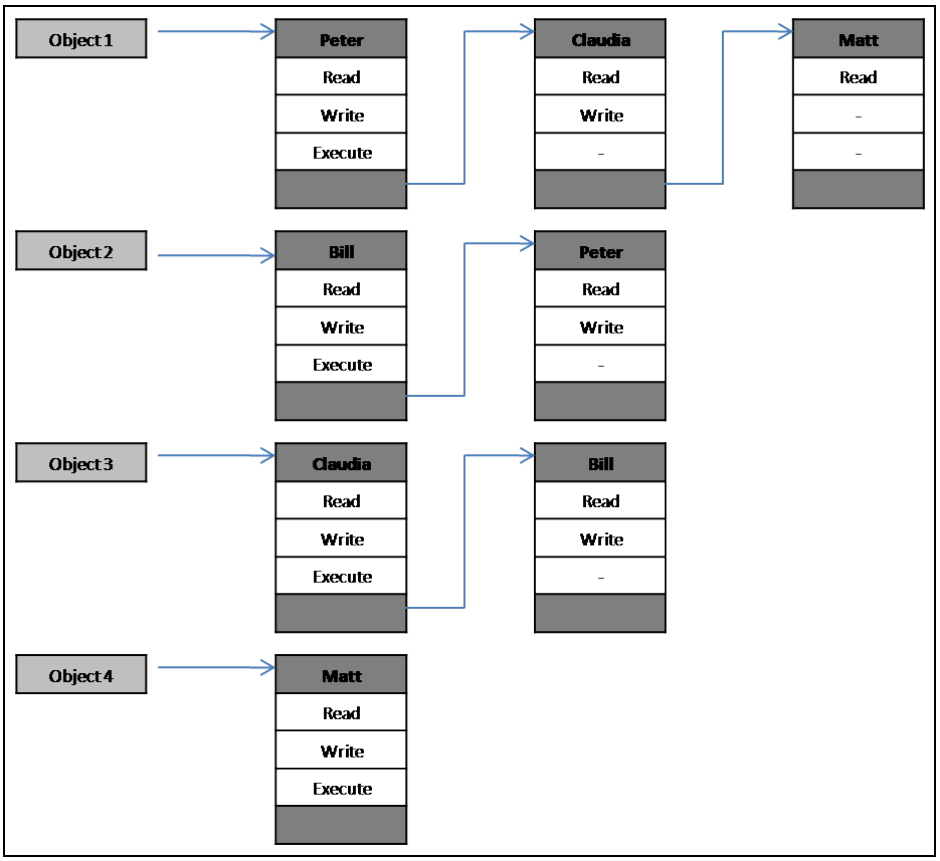


Figure 5.1 Access Control List

A Capability List is used to associate each user with the access permissions to the objects. This is a row wise representation of the access matrix.

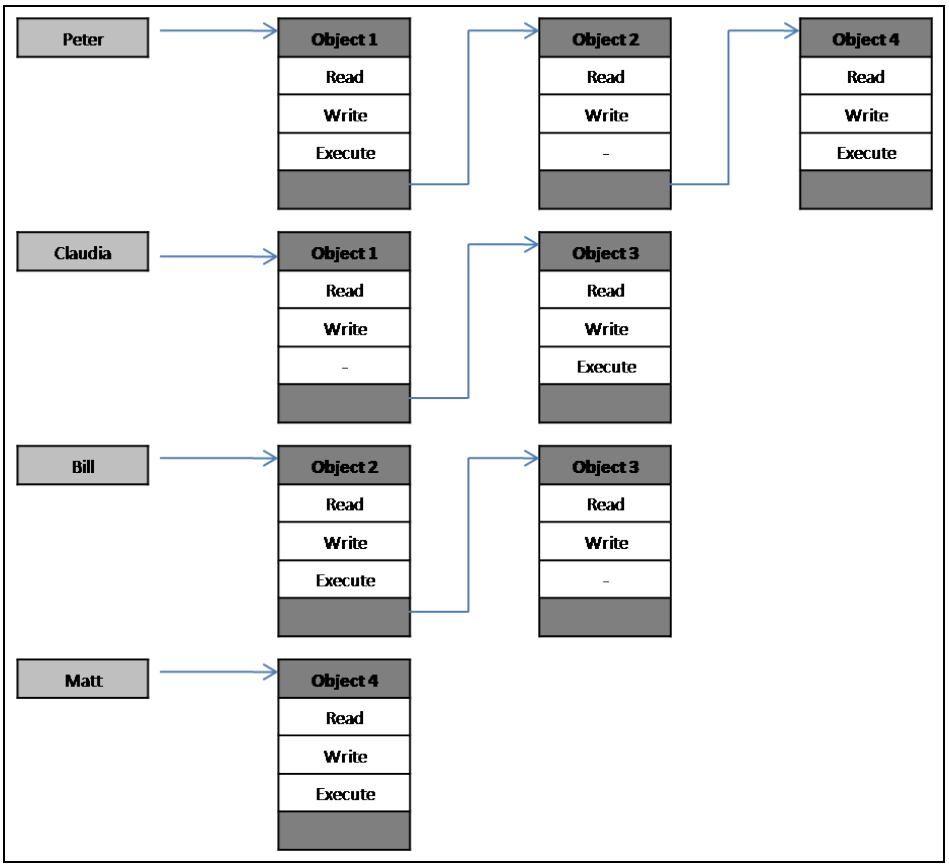


Figure 5.2 Capability List

DAC models have some inherent drawbacks. A significant issue is the fact that a user who is allowed to access an object by the owner of the object has the capability to pass on the access right to other users without the involvement of the owner of the object. This will create inevitable privacy issues if the DAC policy is used in an eHR system. Another factor we have to consider is the ownership of the data. In healthcare we cannot clearly identify a single entity as the owner of health data. An initial argument would be that the patients are the owners of their own health data. But patients are not always health professionals and it is likely that the involvement of, for example, a healthcare authority is necessary. Due to these reasons it is difficult to use only a DAC policy and fulfil access and privacy requirements of all healthcare stakeholders.

Mandatory Access Control

Mandatory access control systems do not consider the requirements of the owners of the data objects (Ferraiolo, et al., 2003). The access to data objects is controlled by assigning a security level to each object and comparing that security level to the user's security clearance and need-to-know. In order to access an object,

the user must possess a clearance that is greater than or equal to the objects classification. In the MAC policy the flow of information from a higher security level to a lower security level is prevented by the "*Read Down*" and "*Write Up*" rules (Sandhu & Samarati, 1994). Similarly the integrity of the data objects can be protected by using the "*Read Up*" and "*Write Down*" Rules.

However, in a healthcare environment, assigning security levels to objects for the purpose of restricting access is not suitable. The same data type may have different sensitivity levels for different consumers or patients. Thus, a more flexible method of defining sensitivity levels must be incorporated to an access control model used for EHRs.

Role Based Access Control

Role base access control (Sandhu, et al., 1996) models use permissions and rights that are assigned to roles in an organisation to control access to data objects. It does not consider the access rights of an individual. Roles are assigned to all individual users in the systems. The users inherit the access permissions assigned to each role. This allows the system administrators to assign users to roles rather than go through the tedious task of assigning access rights to each and every user.

Roles are assigned to users depending on their capabilities and the job requirements within an organisation. Each user must be given the least privilege depending on their job functions. RBAC policy uses the *need-to-know* principle to assign permissions to roles and to fulfil the least privilege condition.

Purpose Based Access Control

According to the OECD guidelines, "the purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose" (OECD, 1980). Purpose-based access control (PBAC) is based on the notion of relating data objects with purposes (J. W. Byun, et al., 2005). These purposes can determine for what reason data is collected and what they can be used for. Much research has been done in this area and most have identified that greater privacy preservation is possible by assigning objects with purposes (J.-W. Byun, et al., 2005; Naikuo, et al., 2007; Ni et al., 2010). However, according to Al-Fedaghi

(2007), purpose management introduces a great deal of complexity at the access control level. Despite the complexity issues with PBAC, it can help capture the reasons for data collection as well as the intentions of the users, which is a vital factor in healthcare information systems where privacy preservation is a must.

5.3 BUILDING BLOCKS OF THE PROPOSED ACCESS CONTROL MODEL

In order to present the protocols that have been developed we first lay the foundations in the form of the following assumptions.

As stated in section 1.1, we assume the existence of a system with comprehensive EHRs of patients. This EHR system acts as a central system which patients and healthcare providers can access through an Internet connection and is maintained by a central healthcare authority. We eliminate the need for localised EMR systems. The basic architecture of the access control model is illustrated in Figure 5.3.

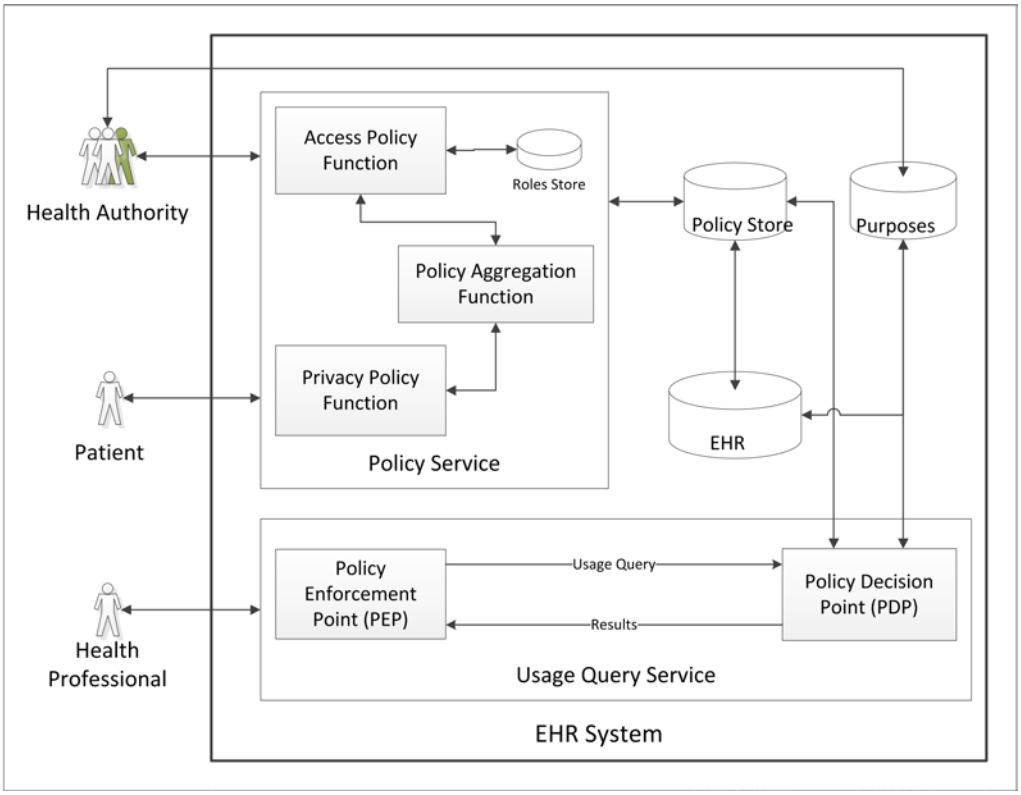


Figure 5.3 Access control model architecture

We have used the terminology used in the XACML standard, policy enforcement point (PEP) and policy decision point (PDP) to have the same meanings. We identify three systems actors; the patient, the preferred healthcare

providers and the health authority. The patients and the health authority formulate the policies associated with each healthcare professional. These policies encompass the requirements of the patients in terms of privacy and the health authority in terms of information requirements.

5.3.1 EHR Data Types and Purposes

The data in the EHR is divided into specific data types and subtypes (Table 5.2) to distinguish between them so that the access and usage policies assigned to them can be directly related to the individual data types with finer granularity. This approach addressed eHealth requirement 5 in section 1.2.6.

Table 5.2 Data types and purposes

Data type	Subtype	*Intended Purpose(s)*
Identity Data	ID1	p1
	ID2	p1
	ID3	p1, p2
General Health	GH1	p1, p2
	GH2	p3, p4
	GH3	p5, p6
Sexual Health	SH1	p5, p6, p7
	SH2	p7, p8, p9
	SH3	p8, p9, p10
Mental Health	MH1	p11, p12
	MH2	p11, p13

Each data type in the EHR is mapped with a purpose(s) for which the data can be used. These purposes relate to healthcare activities that can be performed using the related EHR data element(s). These are called the intended purposes for which data is collected. Similar to Figure 2.3, intended purposes can be, for example, patient visit, referrals, diagnosis purposes, inpatient care, prescribing purposes, sharing, billing, and research. We make the assumption that the intended purposes are comprehensive and current. The central health authority is responsible for the maintenance and update of these purposes. As mentioned in chapter two, the mapping between the EHR data types and the intended purposes will be done with the appropriate domain knowledge. Defining the purposed achieve two things. First, it allows the consumer to know why information was accessed by an HCP at a given time later through audit logs. And helps identify possible misuse of data. Second, it

will prevent HCPs from accessing data without a legitimate purpose, thus acting as a deterrent against misuse.

Definition of purposes and the relevant mapping to EHR data types, without a doubt, is a complex task that requires much care. This process itself has to explore medical knowledge from medical professionals who can identify the significance of a single data element in the care giving process. The data types contain data elements related to them. In a more fine grained level, purposes are related to data elements. For example, Identity Data of a patient can be divided into Name, Date of Birth, Age, Residential Address, etc. The Address can be further divided into street address, Town, State, Country and post code. The more detached the data field gets, the more fine grained it becomes.

There will be a default set of purposes for every data type and elements of that data type. The health authority can define, add and remove purposes related to data types and elements. This will ensure that up to date purposes are maintained in the systems such that the access requirements of care providers are not wrongfully denied. It is understood that the proper definition of intended purposes is a key factor in this model. For the system to reach an optimum performance level it will undoubtedly take time in which initial purpose definitions would be altered and new purposes defined.

5.3.2 EHR data structure

The MAC model grants access to data depending on the sensitivity level of the data elements and the clearance level of the users. But defining the sensitivity level of health information is a complex issue. The sensitivity labelling we use in our approach is different from the classical hierarchical security levels found in MAC (Sandhu & Samarati, 1994). It is difficult to define a clear hierarchical structure for the sensitivity of health data elements that is general to all consumers. For example, sexual health and mental health information may have the same sensitivity for some patients and may not be so for others. If a hierarchical structure is defined, it would be difficult to fulfil certain privacy requirements of patients. We propose sensitivity labelling of EHR data using a tree structure (Figure 5.4) that has the EHR itself as the root element, the data types as children and data elements as grandchildren.

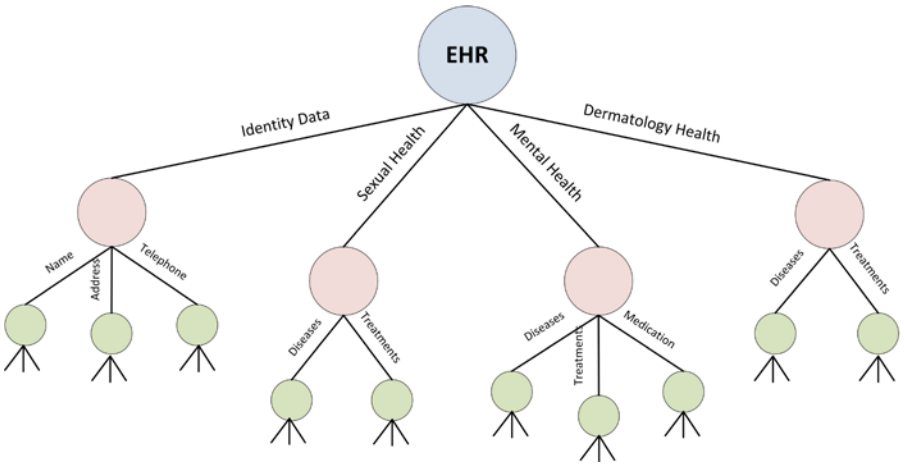


Figure 5.4 Object sensitivity tree

We use a similar technique introduced for purpose representation in Byun et al (Byun & Li, 2008) to represent a sensitivity label of data elements. We refer to this representation as the Sensitivity Tree (ST). A sensitivity label is not assigned to the objects themselves rather we relate the access level of a particular user in terms of the sensitivity label.

Definition 5.1: A sensitivity label (SL) is a tuple <ASL, PSL>, where ASL = [asl_1, asl_2…asl_n] is a set of allowed sensitivity labels and PSL = [psl_1, psl_2…psl_m] is a set of prohibited sensitivity labels.

ASL = [asl_i]; i = 1…n is denoted as all of the descendants of asl_i including asl_i

PSL = [psl_j]; j = 1…m is denoted as all of the descendants of psl_j including psl_j

The definition follows that PSL precedes the corresponding ASL in any specified SL. Therefore, <ASL_X, PSL_X> denotes an SL_Y defined by user "X" for user "Y" with access to all data types included in ASL_X with the exception of data types included in PSL_X. Revisiting the case scenario in section 2.6, we can contextualise the definition of an SL.

Example 5.1: Dr. M can access Patient X's mental health details but cannot access his Sexual or Dermatology details. The access level for Dr. M can be represented in terms of sensitivity labels as follows.

$SL_{Dr.\ M}$ = < [EHR], [Sexual Health, Dermatology Health] >

Here we use the Denial-Takes-Precedence (Bertino, 1998) principle. Access is granted to the entire EHR and then access is denied to specific field by the PSL. This helps isolate the most sensitive information in the EHR that needs to be hidden from

certain users. The access level for a particular user can also be represented as follows.

$SL_{Dr.\ M}$ = < [Identity Data, General Health, Mental Health], [NULL] >

Specifying the data elements that Dr. M can access can be a more tedious task than specifying the data elements he cannot access. We will use this representation to represent the minimum access levels defined by the health authority. The health authority is only concerned with allowing access to particular data fields for the relevant health practitioners. This representation can also be used in purposes such as research where access is required only to a particular data type.

Example: Data of a survey of people who have suffered from some form of a STD during the last 10 years. For this purpose access is required only for the sexual health data type. Under no foreseeable circumstance would there be a requirement for accessing other fields of the EHR. The access level can be represented as follows.

$SL_{Researcher}$ = < [Sexual Health], [NULL]>

Using this method of representing the access levels enables more fine grained control over the data accessed by users that is governed by the SLs assigned for each user. Unlike common access control models, in our approach the permissions and prohibitions are not assigned to the data assets, as mentioned earlier. Our approach eliminates the need for a hierarchical structure for the sensitivity of the data types. Since the data types can be distinguished through the ST, in accordance with eHealth requirement 5, the SLs for each HCP can be defined by both patients and the health authority with high expressive power.

5.4 THE ACCESS CONTROL PROTOCOLS

In this section we shall present the protocols defined to set policies and access data in the EHR. Throughout this section we will use the Specification Description Language (SDL) and Message Sequence Charts (MSC) to graphically present the protocols used in the model. First we will give an overview of SDL and MSC.

5.4.1 Overview of SDL and MSC

The Specification and Description Language (SDL) is a formal language defined by the International Telecommunications Union (ITU-T). It can be used to describe unambiguous specifications and descriptions of the behaviour of real time

systems. A specification of a system is the description of its required behaviour and a description of a system is the description of its actual behaviour. SDL, together with Message Sequence Charts (MSC), can be used to provide a clear description of the behaviour of a system in terms of the behaviour of each individual agent in the system and their communications with each other. Figure 5.5 introduces the SDL notation used in this thesis.

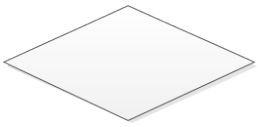
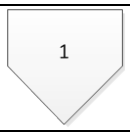
Symbol	Name	Description
	State	This symbol represents a state of the system. The state symbol indicates that the system is waiting to an input.
	Procedure	This symbol represents a Procedure. A procedure contains a description of a system activity.
	Message from User	This symbol represents a message from the user. The messages are considered as inputs to the system.
	Message to User	This symbol represents a message to the user. The messages are considered as outputs from the system.
	Decision 1	This symbol represents a decision by the system. The decisions have specific outputs that trigger events in the system.
	Decision 2	This symbol represents a decision by the system. The decisions have specific outputs that trigger events in the system.
	Off page reference	This symbol represents a reference outside the current page (current SDL diagram).
	Return	This symbol represents a return state. The return state means that the procedure has terminated and returns to the start state.

Figure 5.5 Basic SDL notation

5.4.2 Motivating case scenario revisited

A brief description of the motivating case scenario in section 2.6 is given below that is used to illustrate the access control protocols.

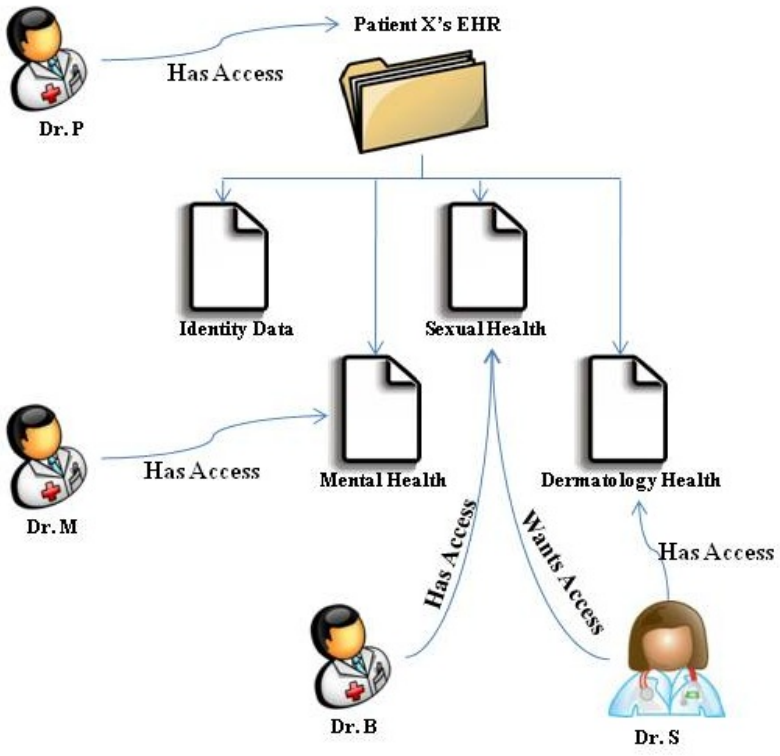
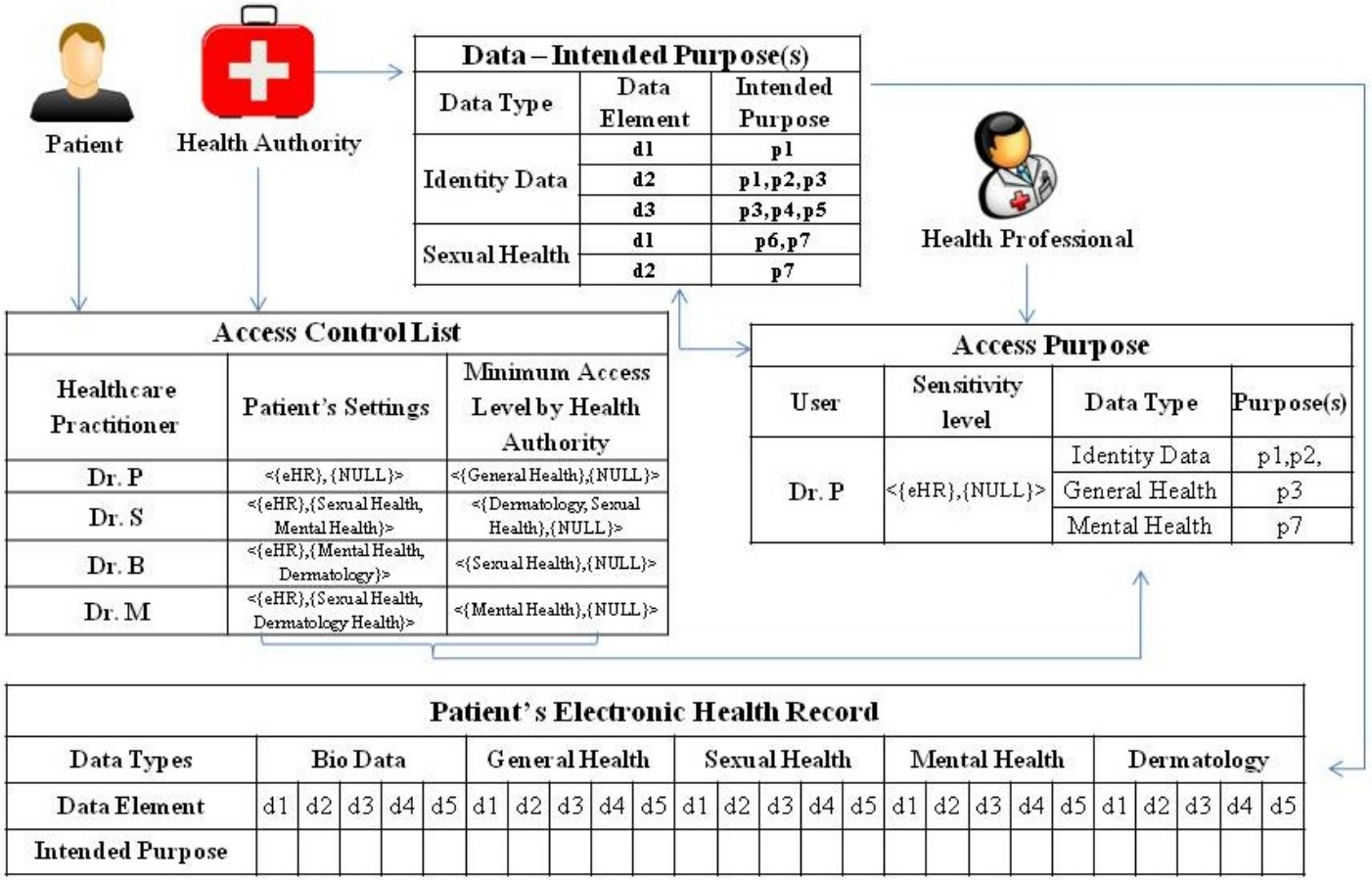


Figure 5.6 Case scenario

Patient X's GP is Dr. P. As his GP, Patient X has allowed Dr. P complete access to the data in his eHR. Patient X has also been treated by Dr. S a dermatologist, Dr. B a sexual health specialist and Dr. M a mental health specialist in the recent past. As a result Patient X allows Dr. B to access his sexual health details, Dr. M to access his mental health details and Dr. S to access his dermatology health details. He does not want Dr. B or Dr. S accessing his mental health details and Dr. M or Dr. S accessing his sexual health details. Patient X suffers from a severe skin disease and does not want either Dr. B or Dr. M accessing his dermatology details due to embarrassment. He is aware that his care providers may need to share his information with other specialists but does not want them sharing the details without his consent. Dr. S believes Patient X's skin condition may be related to a known STD and wants access to Patient X's sexual health details.

5.4.3 Setting Access Policies

In section 1.2.6, we identified two types of requirements that need to be fulfilled. In this section we will show how the policies are set by the actors in our model. An abstract view of the data within the components is given in Figure 5.7.



Data – Intended Purpose(s)

Data Type	Data Element	Intended Purpose
Identity Data	d1	p1
	d2	p1,p2,p3
	d3	p3,p4,p5
Sexual Health	d1	p6,p7
	d2	p7

Access Control List

Healthcare Practitioner	Patient's Settings	Minimum Access Level by Health Authority
Dr. P	<{eHR}, {NULL}>	<{General Health},{NULL}>
Dr. S	<{eHR},{Sexual Health, Mental Health}>	<{Dermatology, Sexual Health},{NULL}>
Dr. B	<{eHR},{Mental Health, Dermatology}>	<{Sexual Health},{NULL}>
Dr. M	<{eHR},{Sexual Health, Dermatology Health}>	<{Mental Health},{NULL}>

Access Purpose

User	Sensitivity level	Data Type	Purpose(s)
Dr. P	<{eHR},{NULL}>	Identity Data	p1,p2,
		General Health	p3
		Mental Health	p7

Patient's Electronic Health Record

Data Types	Bio Data					General Health					Sexual Health					Mental Health					Dermatology				
Data Element	d1	d2	d3	d4	d5	d1	d2	d3	d4	d5	d1	d2	d3	d4	d5	d1	d2	d3	d4	d5	d1	d2	d3	d4	d5
Intended Purpose																									

Figure 5.7 A data representation of the access control model components

Fulfilling the Healthcare Providers Requirements

The healthcare authority will define a role structure of the health organisation and assign the minimum access level for each role in the organisation, thus fulfilling eHealth requirement 1 in section 1.2.6. In this role definition each role will be given a default sensitivity level for data access which will be discussed later. Even though the patients' privacy requirements have to be considered before data access is granted, there is no input from the patient for the default access policy. This phase is purely dedicated to fulfilling the organisational access and policy requirements. In a normal RBAC model, the role of the user has to change when the permissions for the user changes. For this reason only the initial user-role assignment is done using the RBAC method to simplify the tasks of the responsible authority.

Fulfilling the Patients Privacy Requirements

A DAC and MAC type approach is used by the patient to specify who can access his EHR, hence fulfilling eHealth requirement 6. The patient will also define what each HCP can access in his EHR, which fulfils eHealth requirement 7. He will populate an Access Control List (ACL) with the healthcare practitioners who he prefers to be able to access his eHR. The patient also has the capability to specify the access level of each of the users in terms of a sensitivity label in the ACL which is done using the MAC based process. Although eHealth requirement 9 states that the administrative process must be easy to understand, the usability aspects are not addressed here.

Table 5.3 Access control list

Healthcare Practitioner	Patient's Settings	Minimum Access Level Set by Health Authority
Dr. P	<[EHR], [NULL]>	<[General Health],[NULL]>
Dr. S	<[EHR],[Sexual Health, Mental Health]>	<[Dermatology, Sexual Health],[NULL]>
Dr. B	<[EHR],[Mental Health, Dermatology]>	<[General Health, Sexual Health],[NULL]>
Dr. M	<[EHR],[Sexual Health, Dermatology Health]>	<[General Health, Mental Health],[NULL]>

The table above shows an abstract ACL. Patient X has granted 4 health care practitioners access to his EHR. But the access is bound by the patient's privacy settings and the settings by the health authority. The settings by the health authority are set during the role assignment as seen in the previous section.

5.4.4 Internal Protocols

The sensitivity level defined by the health authority is different to what is defined by the patients. PSLs set by the health authority will always be *NULL*. As mentioned above, this is because the health authority is concerned with allowing access to the health professionals. The ASLs set by the health authority does not allow the HCP to access other data types. Explicit prohibitions are defined by the patients. Allowed sensitivity level set by the patients always precedes that which is set by the health authority if there is no conflict between the patients prohibited sensitivity label and the allowed sensitivity label set by the health authority. The allowed sensitivity level set by the health authority always precedes the prohibited sensitivity label set by the patients if there is a conflict. This characteristic fulfils eHealth requirement 4 in section 1.2.6. This will ensure that the relevant information is always available to the right person in terms of providing better healthcare and fulfil the "need-to-know" principle associated with EHRs. A formal definition for this notion is given below.

Definition 5.2:

IF ($ASL_{Patient} \geq ASL_{HealthAuthority}$ AND $PSL_{Patient} \cap ASL_{HealthAuthority} = \emptyset$) THEN $SL_{HealthProfessional} = < [ASL_{Patient}], [PSL_{Patient}] >$

IF ($ASL_{Patient} < ASL_{HealthAuthority}$ AND $PSL_{Patient} \cap ASL_{HealthAuthority} = \emptyset$) THEN $SL_{HealthProfessional} = < [ASL_{Patient} \cup ASL_{HealthAuthority}], [PSL_{Patient}] >$

IF ($ASL_{Patient} \geq ASL_{HealthAuthority}$ AND $PSL_{Patient} \cap ASL_{HealthAuthority} \neq \emptyset$) THEN $SL_{HealthProfessional} = < [ASL_{Patient}], [PSL_{Patient} \cap ASL_{HealthAuthority}`] >$

IF ($ASL_{Patient} < ASL_{HealthAuthority}$ AND $PSL_{Patient} \cap ASL_{HealthAuthority} \neq \emptyset$) THEN $SL_{HealthProfessional} = < [ASL_{Patient} \cup ASL_{HealthAuthority}], [PSL_{Patient} \cap ASL_{HealthAuthority}`] >$

Note: Please note that " ` " indicates complement.

When these conditions are satisfied, the sensitivity levels are updated so that the users can access the relevant data types/elements. E.g. Dr. S (Table 5.3) will be assigned a sensitivity level $SL_{Dr.\ S} = <$ [EHR], [Mental Health]>. Algorithm 1 shows how sensitivity levels are set for the users. The symbols other than the ones used previously denote as follows.P_{SL} and HA_{SL} denote sensitivity levels set by the Patient (*P*) and the Health Authority (*HA*) for a healthcare professional respectively.

Algorithm 1: Policy Aggregation

1: **Input**: 1. User ID: *UID*
2: 2. Health Authority Policy: $HA_{SL\_UID} \leftarrow <ASL_{HA\_UID}, PSL_{HA\_UID}>$
3: 3. Patient Policy: $P_{SL\_UID} \leftarrow <ASL_{P\_UID}, PSL_{P\_UID}>$
4: **Output**: User Sensitivity Label SL_{UID}
5: **Method**:
6: **if** ($ASL_{P\_UID} \geq ASL_{HA\_UID}$ AND $PSL_{P\_UID} \cap ASL_{HA\_UID} = \emptyset$) **then**
7: $SL_{UID} \leftarrow < [ASL_{P\_UID}], [PSL_{P\_UID}] >$
8: **else if** ($ASL_{P\_UID} < ASL_{HA\_UID}$ AND $PSL_{P\_UID} \cap ASL_{HA\_UID} = \emptyset$) **then**
9: $SL_{UID} \leftarrow < [ASL_{P\_UID} \cup ASL_{HA\_UID}], [PSL_{P\_UID}] >$
10: **else if** ($ASL_{P\_UID} \geq ASL_{HA\_UID}$ AND $PSL_{P\_UID} \cap ASL_{HA\_UID} \neq \emptyset$) **then**
11: $SL_{UID} \leftarrow < [ASL_{P\_UID}], [PSL_{P\_UID} \cap ASL_{HA\_UID}\ `] >$
12: **else if** ($ASL_{P\_UID} < ASL_{HA\_UID}$ AND $PSL_{P\_UID} \cap ASL_{HA\_UID} \neq \emptyset$) **then**
$SL_{UID} \leftarrow < [ASL_{P\_UID} \cup ASL_{HA\_UID}] , [PSL_{P\_UID} \cap ASL_{HA\_UID}\ `] >$
13: **end if**
14: **return** SL_{UID}

Note: Please note that " ` " indicates complement.

We will now look at how the sensitivity level for Dr. S, from our case scenario in section 2.6, is set in our model. The steps taken to set the sensitivity label for a dermatology health professional are as follows.

1. A representative from StateHealth creates a dermatologist role definition.
    a. StateHealth initiates the request with the access policy service
    b. The access policy service requests the default sensitivity label for the dermatologists role
    c. StateHealth sends the default sensitivity level
    d. A new dermatology role is created by the access policy service and is stored in its roles database
    e. StateHealth is notified of the process completion
2. StateHealth assigns the role of dermatologist to Dr. S
    a. StateHealth initiates the request with the access policy service
    b. Access policy service requests health professionals credentials
    c. The access policy service requests Dr. S's credentials
    d. StateHealth sends Dr. S's credentials

e. The access policy service assigns a dermatologist role to Dr. S

f. The role assignments data base is updated

g. StateHealth is notified of the process completion

3. Patient X adds Dr. S to his ACL

a. Patient X logs into the EHR system as a patient

b. Patient X initiates a request to add Dr. S to the ACL

c. The privacy policy service request the sensitivity label for Dr. S

d. Patient X sends the sensitivity label for Dr. S to the privacy policy service

e. The privacy policy service sends the privacy policy to the policy aggregator

f. The policy aggregator request Dr. S's default sensitivity label from the access policy service

g. The access policy service sends Dr. S's default sensitivity label from its roles database to the policy aggregator

h. The policy aggregator formulates the final policy for Dr. S

i. The policy aggregator sends the final policy to the privacy policy service

j. The privacy policy service sends the final policy to Patient X and ask for his acknowledgement

If a negative acknowledgement is received;

i. the policy aggregator is notified and the policy aggregator discards the policy

ii. PPS notifies the patient

k. Patient X send a positive acknowledgement to the privacy policy service

l. The privacy policy service sends approval to the policy aggregator

m. The policy aggregator sends the final policy to the policy store

n. The policy store stores Dr. S's sensitivity label as an access policy

o. The PPS sends notification of final policy service to Patient X

The SDL diagrams that correspond to this process are show in the figures below.

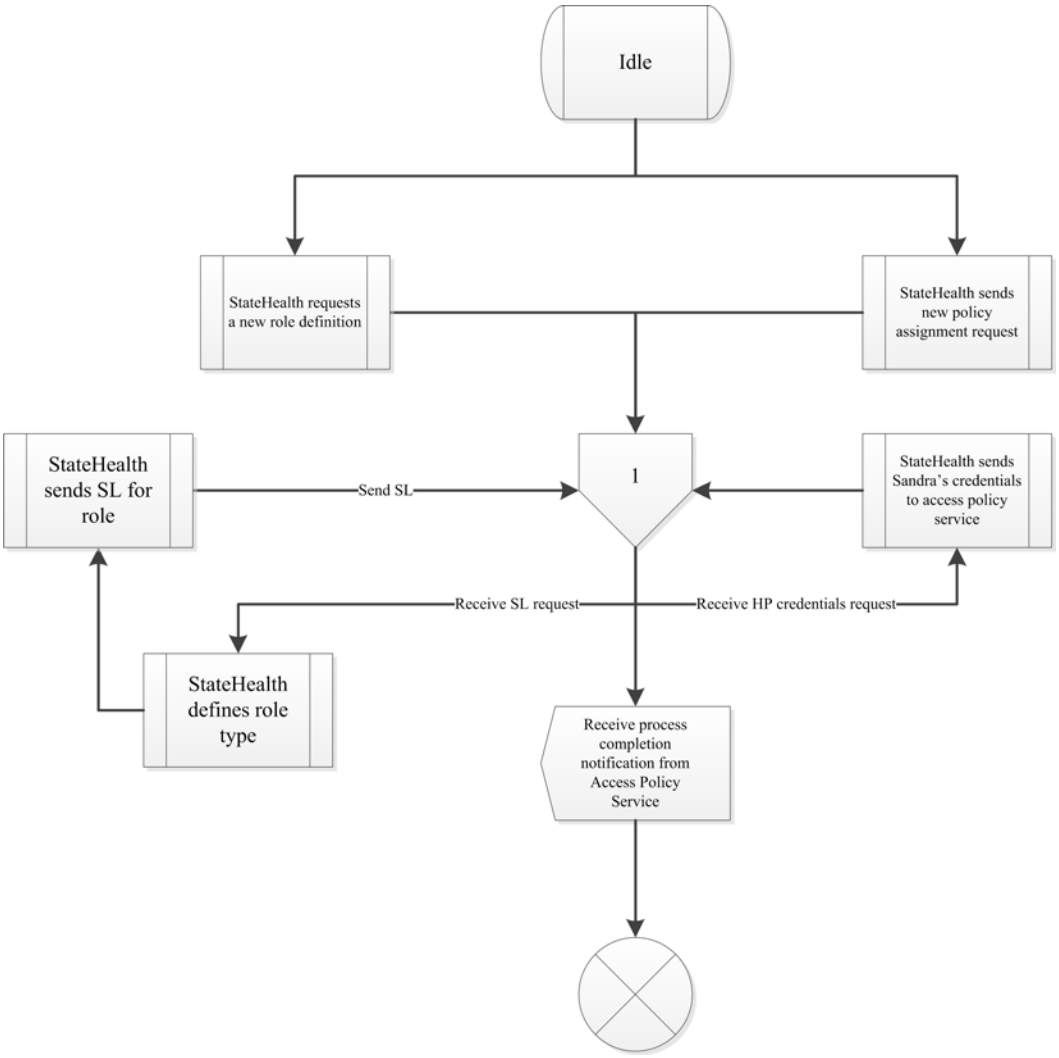


Figure 5.8 SDL for Health Authority

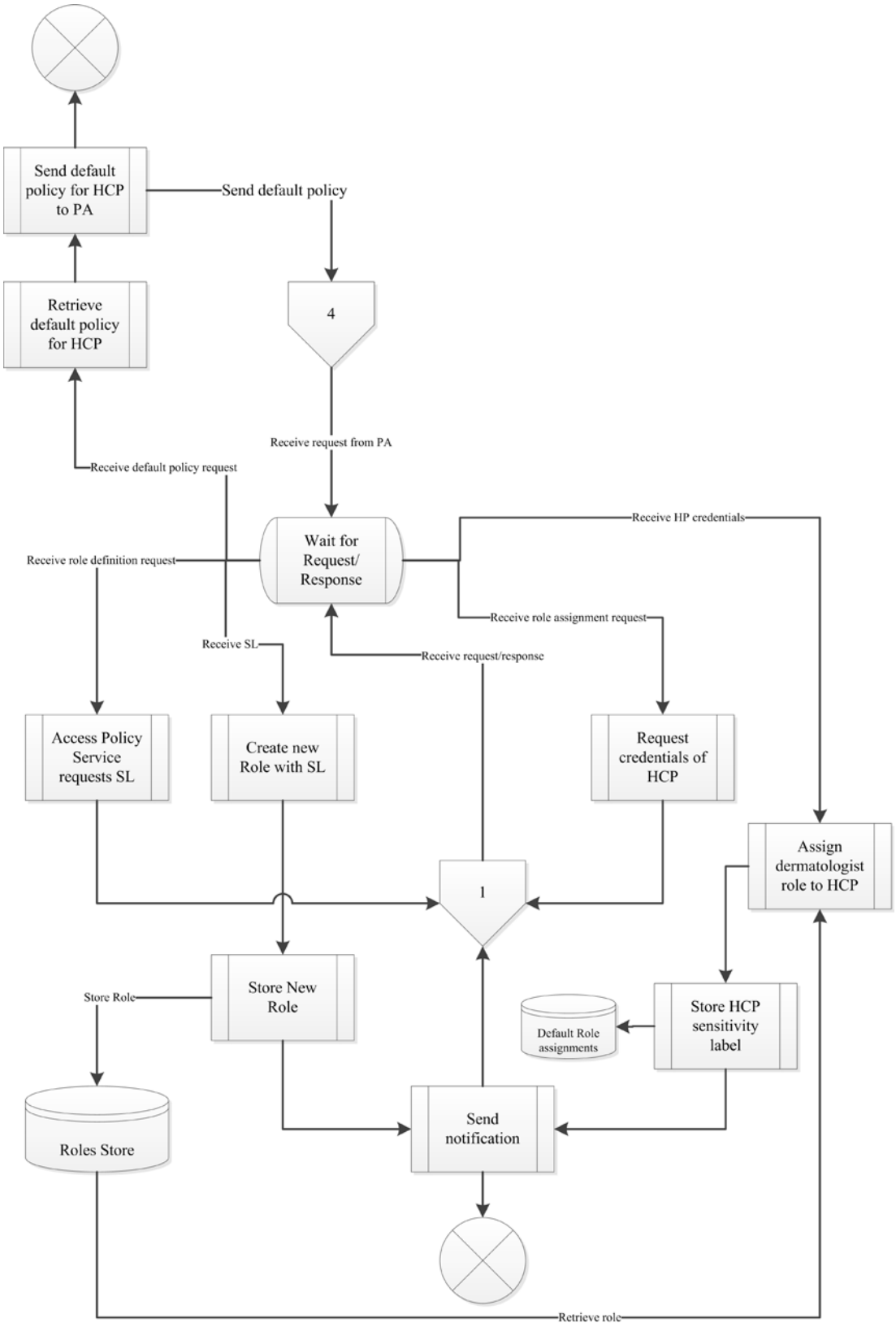


Figure 5.9 SDL for Access Policy Function (APS)

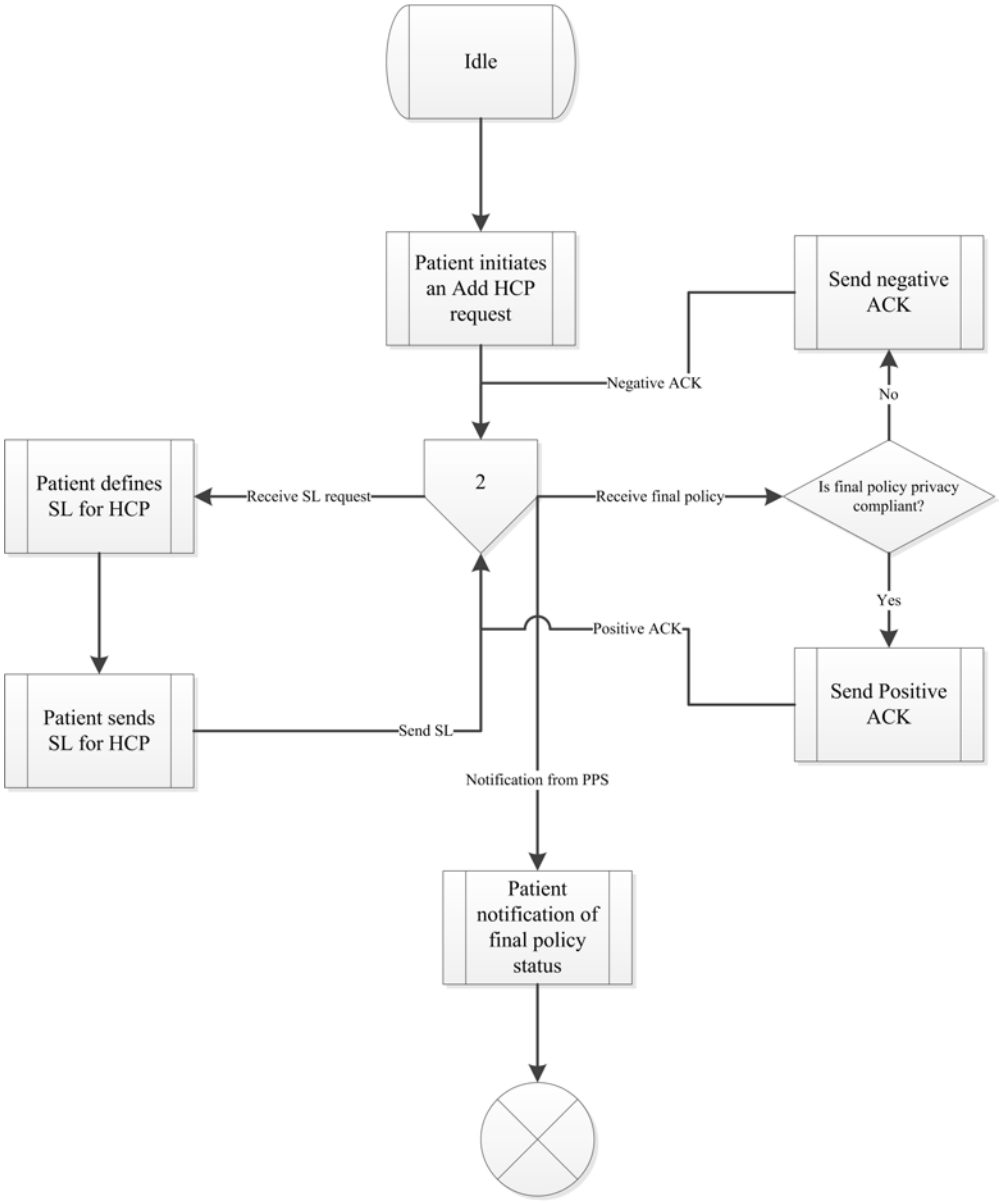


Figure 5.10 SDL for the Patient

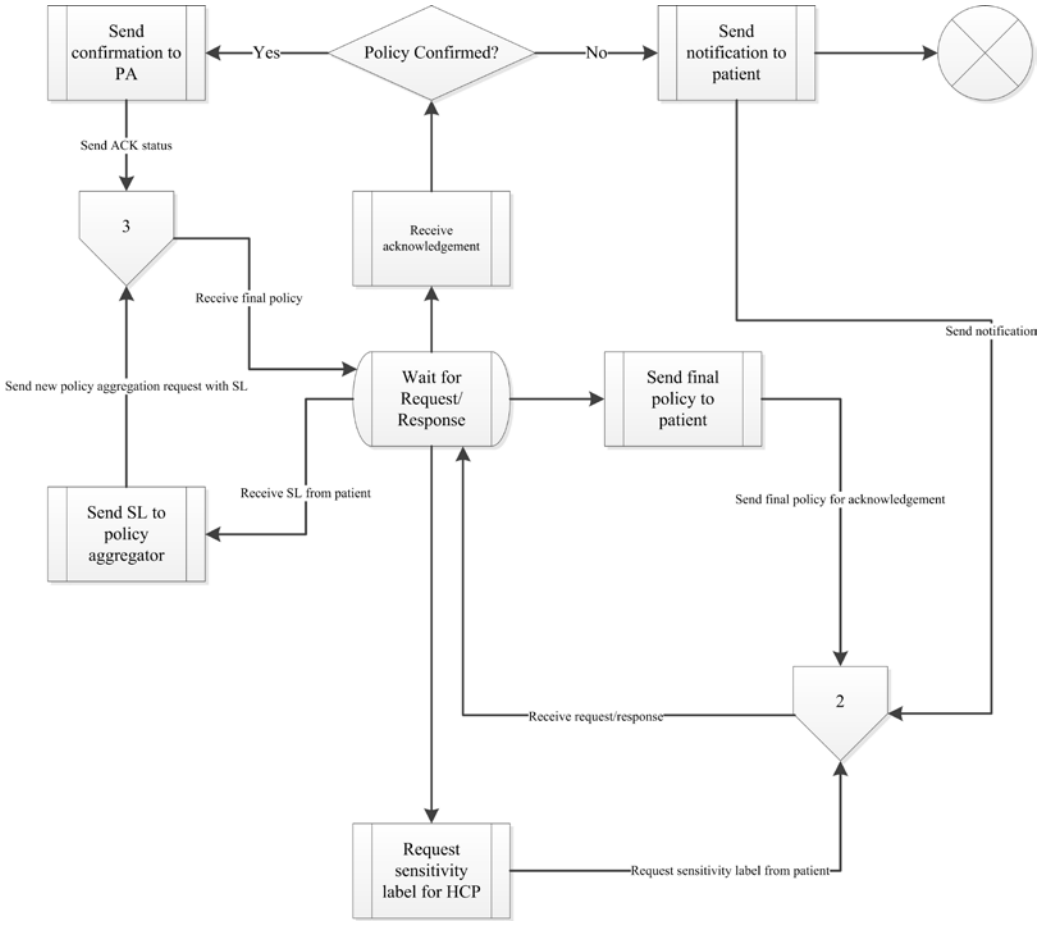


Figure 5.11 SDL for the Privacy Policy Function (PPF)

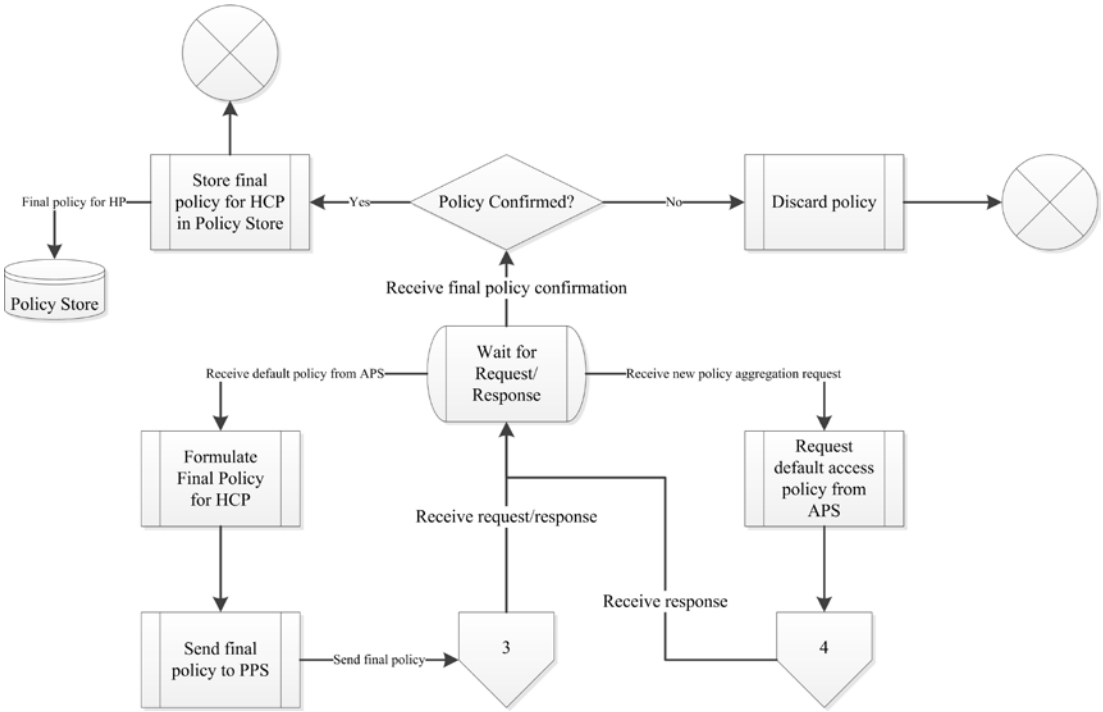


Figure 5.12 SDL for the Policy Aggregation Function

A sequence diagram for this policy setting process is shown in Figure 5.13.

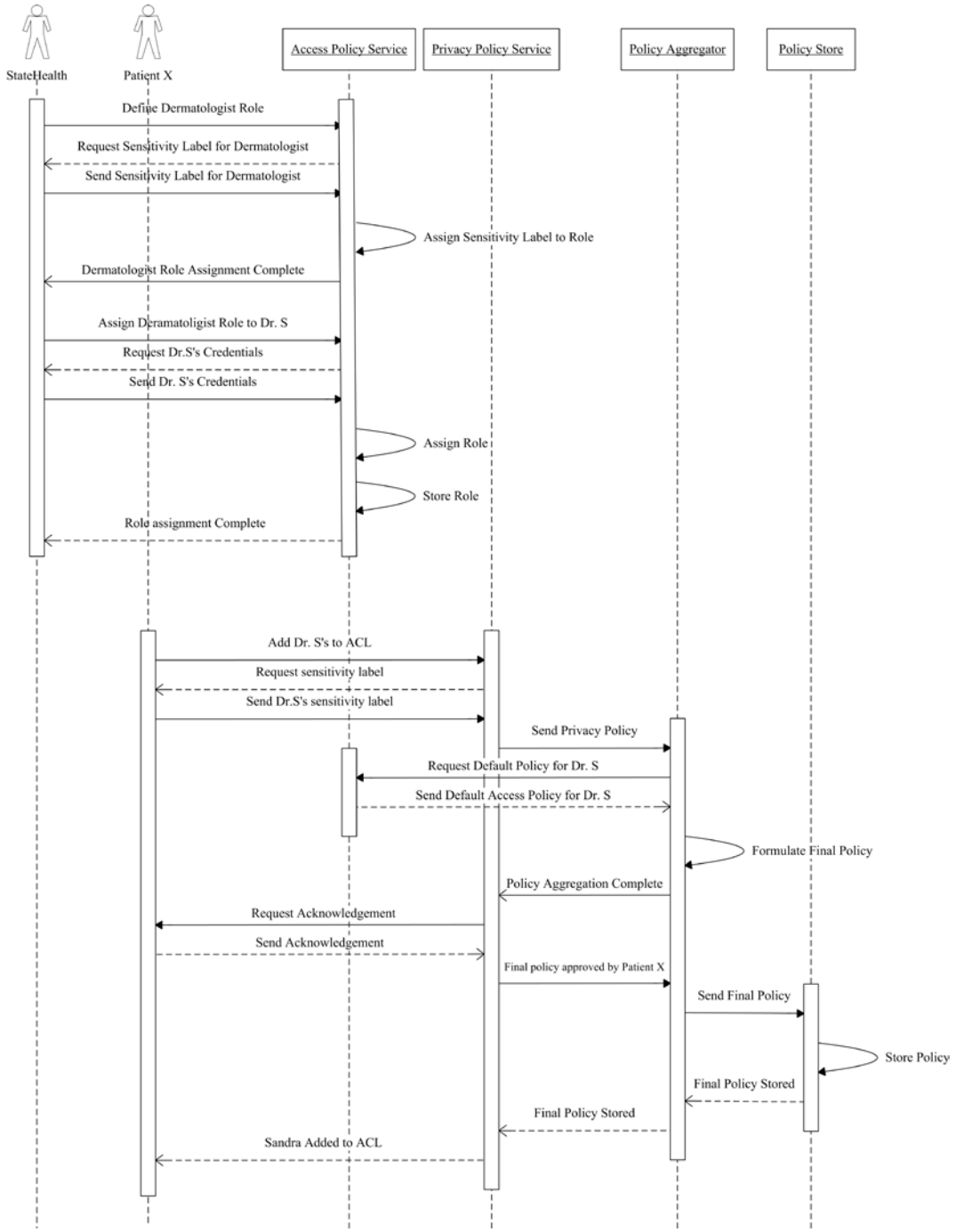


Figure 5.13 Final policy for Dr. S

5.4.5 Accessing Data in the EHR

The health authority defines intended purposes for each data type and element in an EHR. Access requests of authorised users are also handled in a purpose based manner. When a user requires access to data in an EHR they define an access request consisting the reason(s) or purpose(s). This definition will be compared with the purposes in Table 5.2, which were assigned to the data elements by the healthcare authority. If satisfied access is granted. The granular level access to data is granted

depending on the SL of each user. The access purposes are captured for the purpose of identifying the reason for accessing data, which is used for accountability purposes as will discussed in chapter six.

Table 5.4 represents typical access requests by authorised health practitioners. An access request may not particularly be for a single task. Each data type requested may not always be associated with a single purpose. The users must have the capability to specify multiple purposes in a single access request to enhance the ease of use. If access is granted we have to make the assumption that each data element can only be used for the specified access purpose(s). The health information systems which would use this access control model should have the capability to provide the functionality where data misuse can be captured.

Algorithm 2: Access Request

```
1:  Input:  1. User ID: UID
2:          2. Sensitivity Level: SL_UID
3:          3. Access Purposes List: AccPurList[d_AP, p_AP]
4:          4. Intended Purposes List: IntPurList [d_IP, p_IP]
5:  Output: Access_State []
6:  Method:
7:   Num_Requests ← Size (AccPurList)
8:   Num_Pur← Size (AccPurList)
9:   Access_State [Num_Requests] ← False
10:  Permit_Data [Num_Requests] ← False
11:  Check_Purpose [Num_Requests, Num_Pur] ← False
12:     for i = 1 to Num_Requests do
13:             if IntPurList(i) ∈ PSL(SL_UID ) then
14:                     Permit_Data[i] ← False
15:             else
16:                     Permit_Data[i] ← True
17:              end if
18:     for j = 1 to Size(AccPurList(i)) do
19:             if AccPurList[i, j] ⊆ IntPurList then
20:                     Check_Purpose [i, j] ← True
21:             else
22:                     Check_Purpose [i, j] ← False
23:             if [(Permit_Data [i] = True) AND (Check_Purpose [i, j] = True ) = True]
24:             then
25:                     Access_State [i] ← True
26:             else
27:                     Access_State [i] ← False
28:             end if
29:     end for
30:     end for
31:     return Access_State []
```

Algorithm 2 processes the access requests by health professionals. A tuple with data type and purpose is denoted as <*d, p*>. *Permit_Data* [] contains the status (allowed or disallowed) of the data types requested by the user. *Check_Purpose* [*Num_Requests, Num_Pur*] is a 2D array containing the status of the purposes for each the data type requested. The algorithm returns and array *Access_State* [] with the state of each purpose in the access request. *IntPurList* [d_{IP}, p_{IP}] is a 2D array with data types with their intended purposes (set by the health authority). *AccPurList* [d_{IP}, p_{IP}] is a 2D array with the data types and their access purposes (requested by a user).

Table 5.4 Access requests by authorised users

User	Sensitivity level	Data Type (d)	Access Purpose (p)
Dr. P	<[EHR],[NULL]>	Identity Data	p1,p2
		General Health	p3
		Mental Health	p7, p4
		Sexual Health	p5
Dr. S	<[EHR],[Mental Health]>	Dermatology	p8
		Sexual Health	p5

It is important to note that the nature of the healthcare industry forces us to adopt the *break the glass* emergency mechanisms where the patient's health prevails over privacy requirements. Also, usability is a vital part of every healthcare information system. No matter what the underlying principles are, the users, both patients and the healthcare providers must be given simple directions (e.g. menu) where they can set their access settings easily.

The steps for the data accessing process are as follows.

1. Dr. S logs in to the EHR system as an HCP
    a. Dr. S sends the login credential to the EHR system.
    b. The EHR system authenticates Dr. S and creates a new session
2. Dr. S initiates a data usage request with the usage query service of the EHR system
    a. Dr. S initiates a data request

b. The PEP requests the required details from Dr. S in the form of a usage query

c. Dr. S sends the usage query

d. The PEP sends the usage query to the PDP

3. The policy decision point validates the usage query

a. The PDP checks Dr. S's sensitivity level with the policy store

i. If the sensitivity label is incompatible the sequence ends here and a denial response is sent to PEP and go to step 4b

b. The PDP checks the usage purposes in the usage query with the purposes store

i. If the purpose(s) are invalid the sequence ends here and a denial response is sent to PEP and go to step 4b

c. If steps (a) and (b) are satisfied the PDP fetches the EHR data from the EHR store and sends it to PEP and go to step 4a

4. PEP sends query result to Dr. S

a. PEP sends EHR data to Dr. S if query is policy compliant

b. PEP sends a denial notice to Dr. S

The SDL diagrams for the agents in this sequence are given below.

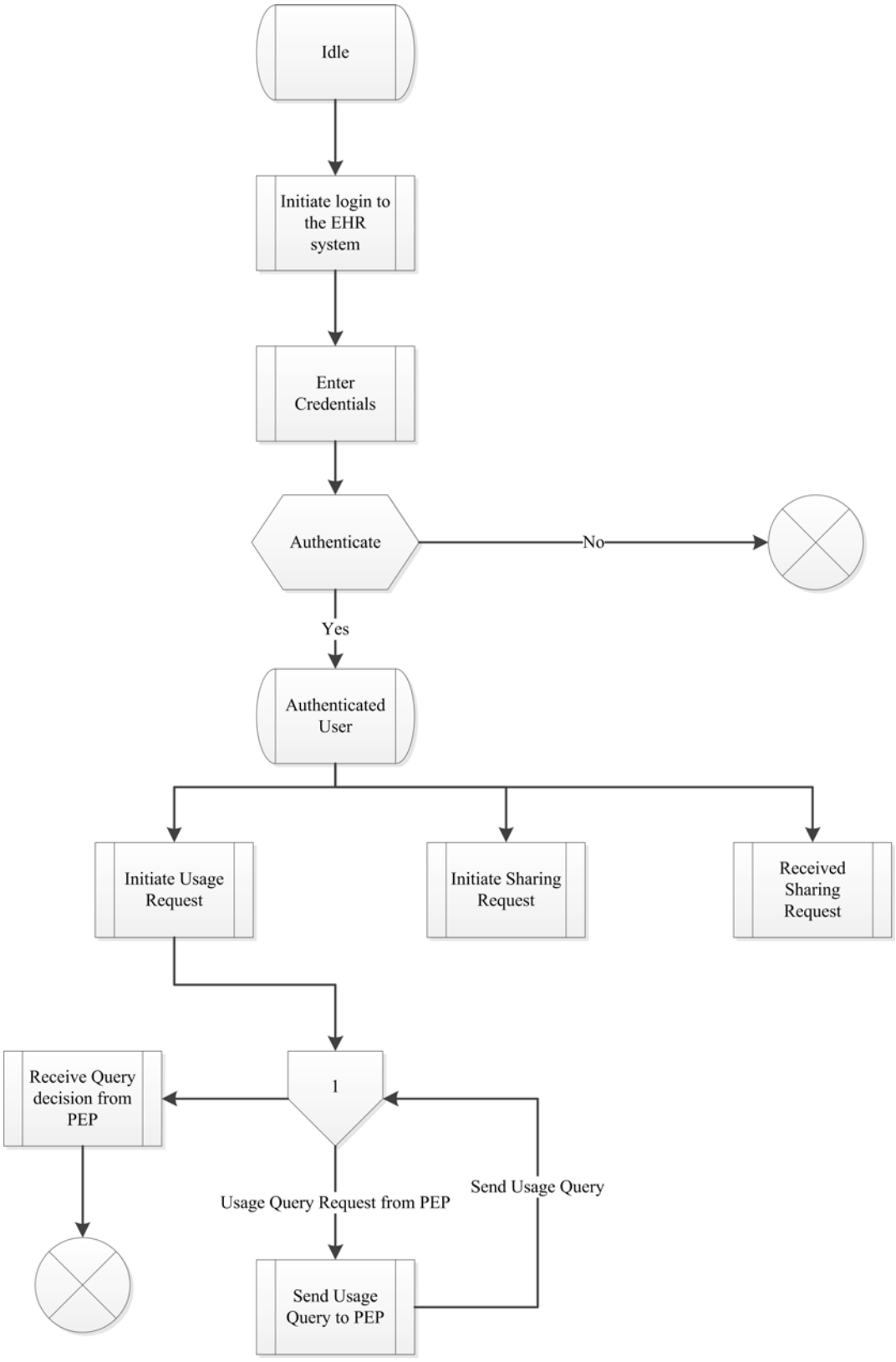


Figure 5.14 SDL for HP Service

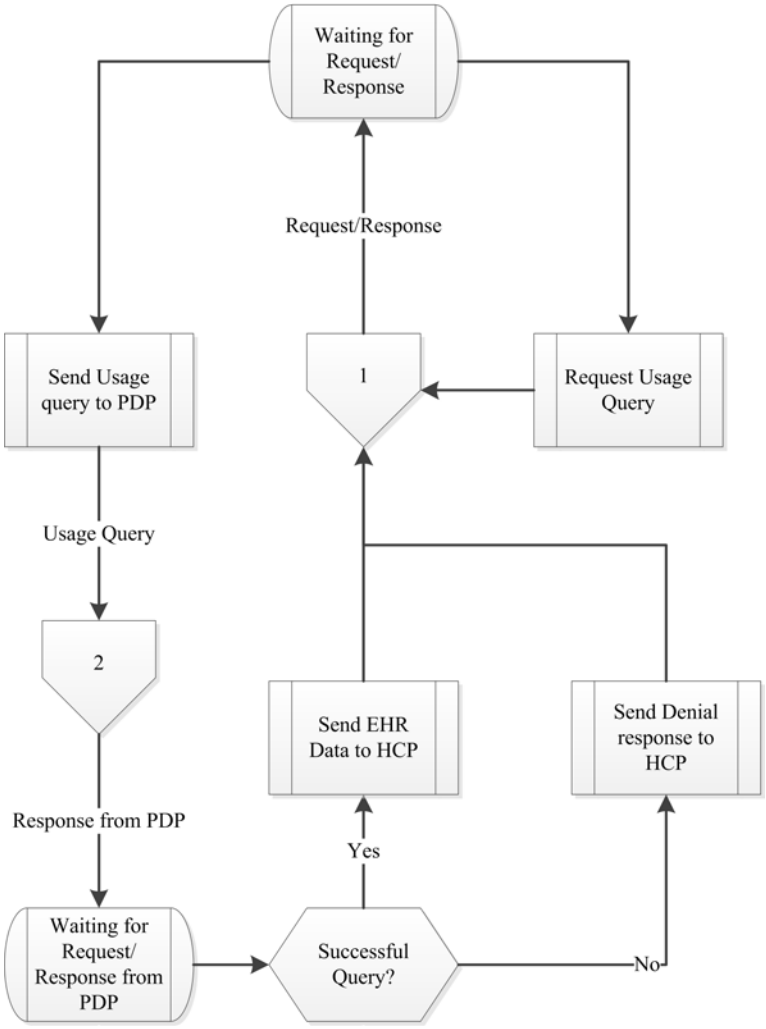


Figure 5.15 SDL for policy enforcement point (PEP)

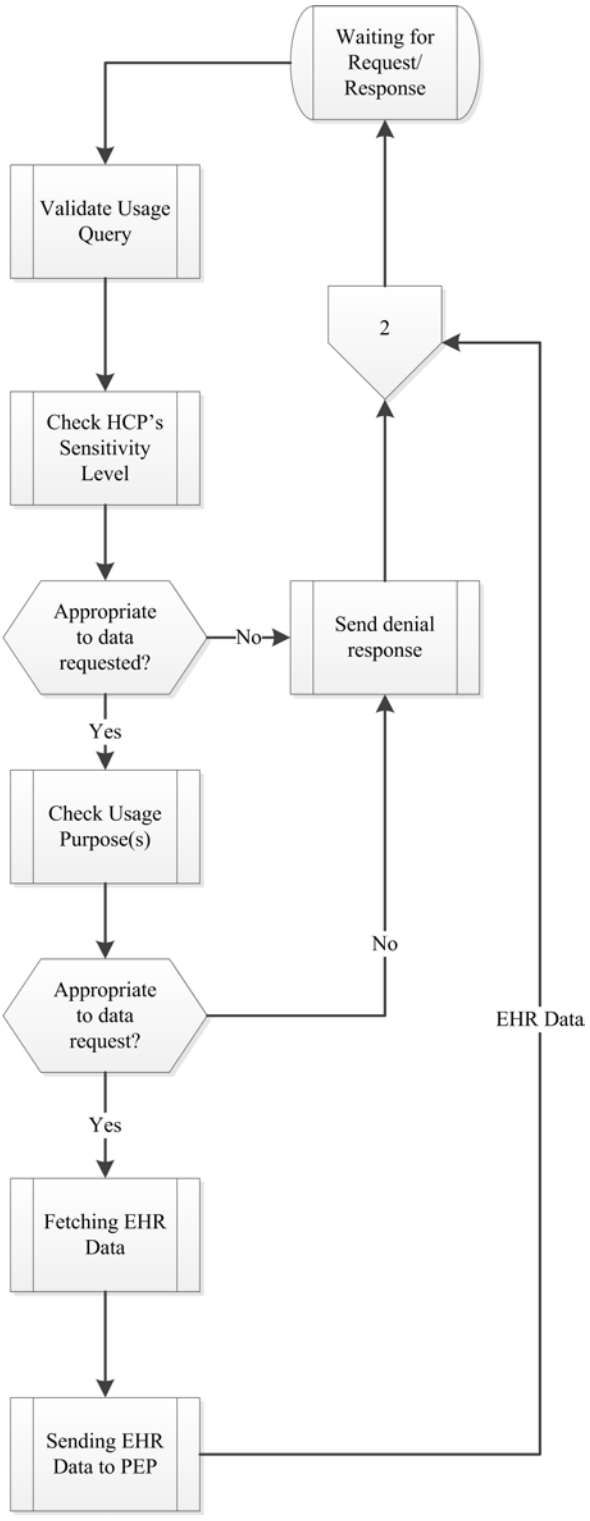


Figure 5.16 SDL for policy decision point (PDP)

A sequence diagram for this process is shown in the Figure 5.17.

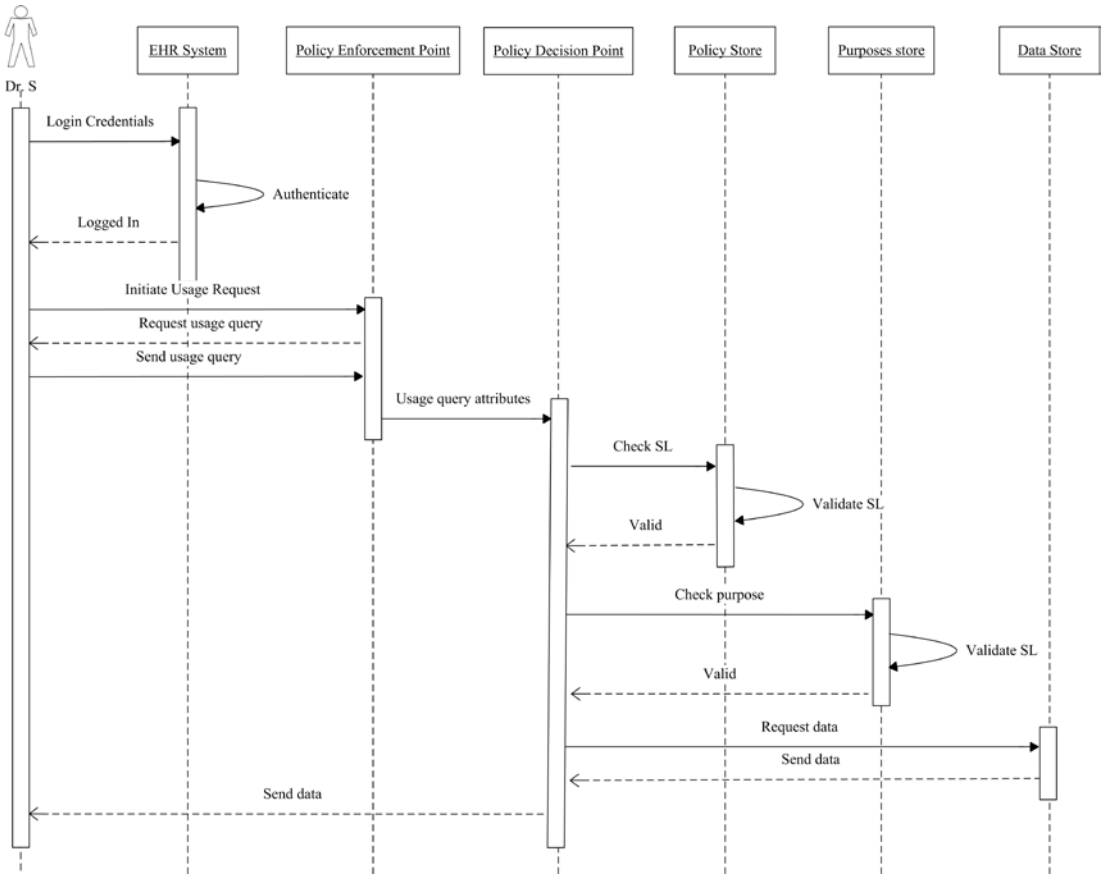


Figure 5.17: Usage request and data retrieval

5.4.6 Information Sharing Example

In our case scenario let us assume that Dr. P, using the PBAC module defined within the portal for authorised users, initiates a request to share Patient X's sexual health details with another health professional Dr. C for the benefit of Patient X. This capability fulfils eHealth requirement 3 in section 1.2.6. Here however, Dr. C should have the relevant access clearance by the health authority to access the type of data specified by the requester. This default access level is set using the RBAC and MAC modules of the access control model. It is not necessarily required that the receiving health professional be in Patient X's ACL which is defined by Patient X through the DAC and MAC modules since it is a request by an authenticated user. It is important to note that Patient X's consent for sharing information is already given to Dr. P by the policies set by the patient and the health authority. Patient X can give any health professional the right to share his health information without his consent with other health professionals. If Dr. C accepts the request she becomes an authorised user of the system with the relevant access level. Patient X has the right to remove Dr. C from the ACL at a later time. Patient X is notified of the actions of the users at

relevant times to make the system transparent. It is important to note that information is shared for the benefit of the patient. Information must not be misused by the users. Trust plays a major role in the information sharing process. Furthermore, such processes are traceable and accountable. An EHR system using this protocol must have the capability to prevent users from misusing information, which is discussed in chapter six.

5.5 A PROTOTYPE IMPLEMENTATION

A prototype of the proposed access control model was developed. The prototype is a Web based system developed using PHP aimed at testing the presented protocols. This implementation is focused only on demonstrating the proposed access control protocol. We are not focused on actual system usability at this stage. Figure 5.18 shows a portion of the prototype that allows patients to set and manage their privacy policies and healthcare professionals to access EHR information. The prototype serves two main purposes: it acts as a test vehicle for the policy formulation and manipulation process described in chapter five and six, and it demonstrates the policy representation that is discussed in chapter six.

The prototype is developed to handle three types of users: patients, a healthcare authority and healthcare professionals. The patients and the healthcare authority can set privacy and access policies and the final policies are formulated according to the protocol discussed above. A MySQL database is used to hold the policies and the data in the EHR. The relationships between the EHR data and the intended purposes are also maintained in this database. Healthcare professionals can lodge access requests that consist of access purposes and will be processed according to the protocol using the intended purposes managed by the health authority. The prototype adheres to the SDL specification given earlier in the chapter and is also capable of handling information sharing processes.

For further clarity of the operations of the prototype, we relate it to our case scenario presented in chapter two. First, Dr. P, Dr. S, Dr. B, Dr. M, Dr. C and all other HCPs who are under that jurisdiction of *StateHealth* register as HCPs by specifying their healthcare role, e.g. General Practitioner (GP), Dermatology Specialist, Sexual Specialist, and Mental Health Specialist. Once an HCP registers in the system, StateHealth is notified. At this point a representative of StateHealth

processes each registration by assigning a default access policy for each of the HCPs. For example, Dr. P will be assigned the role of a GP and Dr. S will be assigned the role of a dermatologist. The policies will contain all required access levels for each healthcare role. This activity fulfils eHealth requirement 1 in section 1.2.6. Once *StateHealth* completes the registration of a HCP, that HCP becomes available for patients, Patient X in our case scenario, to be added to his/her ACL to have access to their EHRs. Patient X selects the HCPs whom he/she wants to have access to his/her EHR, and defines his/her privacy policies for each of them, thus fulfilling eHealth requirements 6 and 7. Before the policies are finalised (i.e. before an HCP is added to the patient's ACL), the privacy policy defined by Patient X for Dr. S will be compared with the default policy defined by *StateHealth* for Dr. S. The policies are amalgamated according to Algorithm 1. If conflicts exist, Patient X is notified before Dr. S is added to his/her ACL to give him/her the option to alter the policy or select a different HCP. The healthcare access policies set by *StateHealth* will prevail over the Patient X's privacy policy such that healthcare information requirements are not hindered, thus fulfilling eHealth requirement 4 in section 1.2.6. Once an HCP is included in Patient X's ACL, he/she can lodge usage requests to access information in Patient X's EHR. Each access request is accompanied by the access purpose specified by the HCP. Access is granted by comparing the access purposes and the intended purposes in the database. We assume that *StateHealth* manages an up-to-date list of purposes associated with each EHR data type.

The access policies that are defined in each of the SLs assigned for the HCPs cannot be overridden by the HCPs in the current state of the prototype. This capability is implemented in the extension of the prototype discussed in chapter six, which also uses a rights expression language for the formal representation of SLs. A detailed description of the policy formulation, representation and manipulation process is given in chapter six.

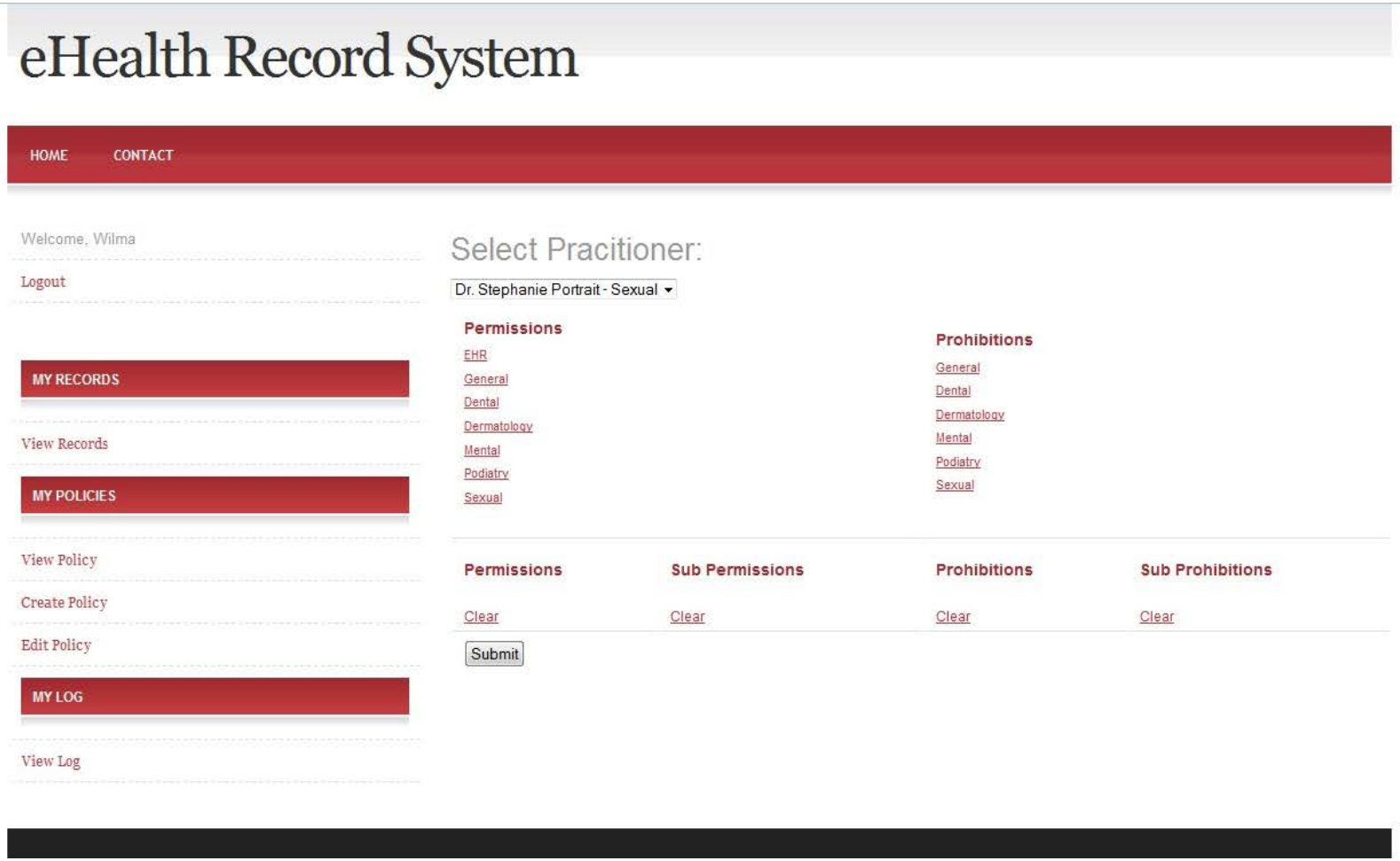


Figure 5.18 Prototype for access control model demonstration

5.6 DISCUSSION AND CONCLUSION

Access control has been a fundamental security measure of information systems for many years. Amongst many different models DAC, MAC, and RBAC are the most popular. These models come in many different variations and are used in different contextual domains. In this chapter we discussed how we can make use of the characteristics and principles of these models to facilitate a suitable access control model for electronic health records. eHealth requirements of eHealth stakeholders identified in chapter two were addressed using the novel access control model that used characteristics of prominent access control models. A DAC based model is used to capture the access settings for users by patients. Patients maintain an ACL of their trusted health professionals and use a variation of the MAC model to assign access levels (or sensitivity level as discussed above) for them. A MAC based model is used to define access levels of healthcare professionals who can access data in an EHR. A central health authority uses a RBAC approach and the MAC based approach to set default access levels for health professionals. A simple PBAC approach is used as a usage control module to capture the access purposes of information users. The current prototype is capable of demonstrating the process of setting the access levels by the patients and the health authority and processing access requests by health professionals. We have tested the prototype to demonstrate various scenarios of policy settings and data access. Further development and testing is required to investigate how this model would behave in a real healthcare setting. Rather than being used as a standalone security model, the final goal of this model is to harmonise the access control model with the information accountability framework (IAF) for eHealth. The IAF uses DRM technologies to represent the access and usage policies set by the users in a Rights Expression Language.

A Web based prototype of the designed model was implemented and tested in different scenarios and the access control protocols were successfully validated. The results of chapters three and four revealed favourable results towards aspects of the designed access control model such as patient control of health information, which further validates the underlying concept. Although presented separately, the access control mode is not intended to be used on its own without the accountability measures presented in chapter six. It is a means of gathering the requirements for AeH systems and supports the model presented in chapter six.

Further to what has been discussed in this chapter we propose the following additions. Purpose definition is an important part in our model. Building a comprehensive set of purposes and maintaining them is vital. These definitions must capture medical knowledge as well as system requirements. The health details of family members and relatives are an important resource for the caring professional. These additions are left for future work to be addressed once a prototype of the IAF is implemented to be tested in a real life healthcare setting. We also extended the proposed model to support explicit actions and providing non-restrictive access to health information for the authorised persons while incorporating information accountability so that health information would not be used inappropriately.

Chapter 6: An Architecture and Policy Framework for Accountable-eHealth Systems

In this chapter, we present and validate a technical architecture and a policy framework for Accountable-eHealth systems. The components of the architecture are focussed towards the policy manipulation of AeH systems thus do not focus on external communications with other aspects of operational system components. The chapter clearly demonstrates the policy protocols presented in chapter five through policy representation and manipulation using a rights expression language, the Open Digital Rights Language (ODRL). The designed architecture is validated using an extension of the prototype developed in chapter five to handle the ODRL policies and transaction logs to demonstrate the operational capability of the model and a model checking approach to validate the internal communications of the architecture. The chapter will also include a detailed account of how the presented eHealth model can be technically implemented using available technologies. Research objectives 3 (b) and 3 (c) are addressed in this chapter.

6.1 INTRODUCTION

eHealth systems are built on Web architectures. The vulnerability of the information in the system depends on how secure the architectural elements of the system would be. When dealing with the use of information within the system we make the assumption that the architectural components that the system is built on are secure. Therefore, the IA principles for eHealth have to be integrated in to the secure architecture on which the systems are built.

The existing concerns in healthcare information management such as information security and information privacy become paramount issues with the use of the Internet to manage health information. This raises questions as to what the relevant security measures are and how an assurance of privacy can be given to the stakeholders (consumers and healthcare professionals).

Unlawful disclosure of personal information contained in EHRs could cause the subject of the information embarrassment and may affect insurability, child

custody cases, and even employment (Cannoy & Salam, 2010; W. Pratt, K. Unruh, A. Civan, & M. M. Skeels, 2006b). To this end, we have already established that a certain degree of control must be given to the patients such that their privacy requirements can be expressed in the form of information privacy policies. A considerable degree of control over ones personal information is an essential aspect to protecting information privacy (Daniel J. Solove, 2008). But, due to the disparity of data ownership in healthcare, giving control of the data must be handled with care.

Various methods have been proposed to address the privacy conundrum ranging from strict access control to privacy-preserving algorithms. From what was discussed section 5.2.1 in chapter five, we establish that access control mechanisms either permit or deny access, there are no intermediate states (Kagal & Pato, 2010). They may also hinder the actions of legitimate users of an information system (Kagal & Pato, 2010). Therefore, relying solely on access control mechanisms to protect sensitive information would be inadequate for privacy protection (Kagal & Abelson, 2010).

In this chapter, a mechanism for information privacy is presented that is neither a preventive nor proactive approach but a non-restrictive and reactive approach. As established in chapter two, the presence of information accountability can deter users from unlawful acts due to the fear of penalties.

6.2 RELATED WORK

Privacy preservation in eHealth is a highly active research area. As it has been pointed out in section 1.2.5, they encompasses issues such as anonymity, authentication, authorisation, confidentiality, deniability, unlinkability and EHR data structure (Slamanig & Stingl, 2010). Despite these efforts, information privacy still hinders the proliferation of eHealth systems. Anonymisation (Bayardo & Agrawal, 2005; Sweeney, 2002) is the property of not being identifiable with respect to a set of actions inside a group of people. In relation to EHRs, anonymity has been defined in terms of anonymous communication, sender-receiver-anonymity and data anonymity (Slamanig & Stingl, 2010). Although in some circumstances these types of anonymisation are appropriate, they may discourage honest and legitimate users from accessing data required to fulfil genuine tasks and also hinder the physician-patient relationship. Deniability refers to the capability of a person to deny the existence of

specific information. This may be applicable in situations where the disclosure of sensitive health information is not a requirement (i.e. non-healthcare related activities). It is stated that deniability should be a capability provided for the users of an EHR system (Slamanig & Stingl, 2010). However, this requirement does not entirely apply when dealing with information manipulation within the healthcare domain. Issues such as unlinkability, which refers to the links with data objects within an EHR, are also not significant in a system that is transparent and accountable. The structure of the EHR play an important role in the authorisation process (Slamanig & Stingl, 2010) (see chapter five for the structure used in this study).

Haas et al. (2011) present a model that addressed privacy aspects of a centralised EHR system. They use digital watermarking to address privacy issues arising from enterprises disclosing health information to third parties such as other doctors, healthcare service providers and drug stores. They propose a model where patients are allowed to express their preferences when disclosing their information to third parties. Their model prevents an organisation providing EHRs from accessing the health information and also prevents them from establishing a profile about the patient. Their model however is not related towards day to day EHR access of healthcare professionals towards healthcare delivery to the patients.

A privacy preserving EHR model has been proposed by Demuynck et al. (2005) which allows patients to control who has access to their EHRs by maintaining a private key. Only the doctors who know this key may access the EHR data and without this the different health records cannot be linked together. Their model also allows doctors to be anonymous when interacting with the central authority only revealing the doctors status. Although patients can control access to their EHR, they cannot prevent them from accessing specific fields of the EHR. They also assume that the healthcare professionals do not misuse the system. This model for privacy management therefore, does not allow for patient requirements as identified in chapter five. It also does not address data misuse that can occur from within the system.

Information accountability is not extensively studied in the eHealth domain. Work by Ferreira et al. (2003) focus on the hardware security appliance (HSA) model to ensure that the accountability data such as audit logs cannot be altered by

system operators such that the integrity of the system is maintained. Their focus is not on patient privacy policies nor is it patient centric. More recently, one study that uses information accountability principles for privacy management in EHRs was proposed by Mashima et al. (2012; 2012) that describes accountable update, accountable use and protection of honest entities of EHRs. In their approach, the authors assume the presence of a monitoring agent that the users interact with for the activities with the EHR system. Although the system is patient centric, it does not describe the involvement of the patient in the policy formulation process nor does it include details of redress in the event of a policy violation. Although the system adopts information accountability for privacy management, the system is not entirely non-restrictive.

Policy override is considered an important aspect of healthcare information systems. With similarity to our work, Ferreira et al. (2006) presents a system where healthcare professionals can override policies within a hospital setting. The system notifies the users when they are about to override a policy to avoid unintentionally accessing the wrong data. At the time of overriding the policy, the users must provide a valid reason for the action. All policy overrides are notified to a relevant supervisor. The fact that healthcare professionals have to provide a justification before they override a policy restricts their freedom to a certain degree. In their approach patients' are not capable of expressing their privacy policies. Their access policies are formulated by a system administrator by considering only the organisational aspects. A similar approach to this has been presented by Weber-Jahnke and Orby (2012). They develop a system to preserve privacy in peer-to-peer exchange of medical information. They consider the patient's consent in their policies.

Our approach in the utilisation of information accountability in healthcare involves several additional aspects than what is already done in that area. Our approach is towards EHRs rather than local EMR systems, which are becoming the most targeted aspect of current eHealth solutions. We clearly show how patients can express their own privacy policies. In our approach, these policies are overlooked by a healthcare authority to guarantee that legitimate healthcare professionals have the appropriate access to the relevant healthcare information. This aspect is not present in previous approaches. In situations where policies are overridden, the patients are

notified. Additionally, they are allowed to directly interact with the healthcare professional to resolve possible disputes resulting in greater transparency that also act as an incentive for healthcare professionals to abide by the rules, which in turn would increase patients' confidence in the system. We also show how the said policies can be formally expressed and managed. Our approach deals with after-the-fact accountability to maximise the availability of information to the healthcare professionals, which is the primary goal of EHRs.

6.3 TECHNICAL ARCHITECTURE FOR AeH SYSTEMS

In the previous chapter we presented and validated an access control model suitable for eHealth systems which capture requirements to fulfil accountability capabilities in an eHealth application domain which utilise a central EHR system. Here we present a technical architecture for AeH systems. It can be considered as an extension to the access control model described above. The policies defined in the access control model act as the underlying policies to which the users must comply to but do not prevent users from accessing data. This is to facilitate unrestricted access to health information for authorised users as mentioned in eHealth requirement 2 in section 1.2.6. Active and user accessible policy-aware transaction logs and after-the-fact inquiries and justifications are introduced to the eHealth domain that facilitate for information accountability.

Prior to presenting the designed model, it must be stressed that functionalities such as the availability of the system, the confidentiality of data transmission between users and the system, and the integrity of the stored data are crucial for any EHR system (Slamanig & Stingl, 2010). It is therefore assumed that the architecture is built upon a secure and trustworthy central EHR system that is managed by a central healthcare authority.

6.3.1 Accountable-eHealth System Architecture

Here, we present a technical architecture for the accountability model seen in chapter two Figure 2.5 that support the accountability capabilities. The access control model presented in chapter five is extended and additional components are introduced.

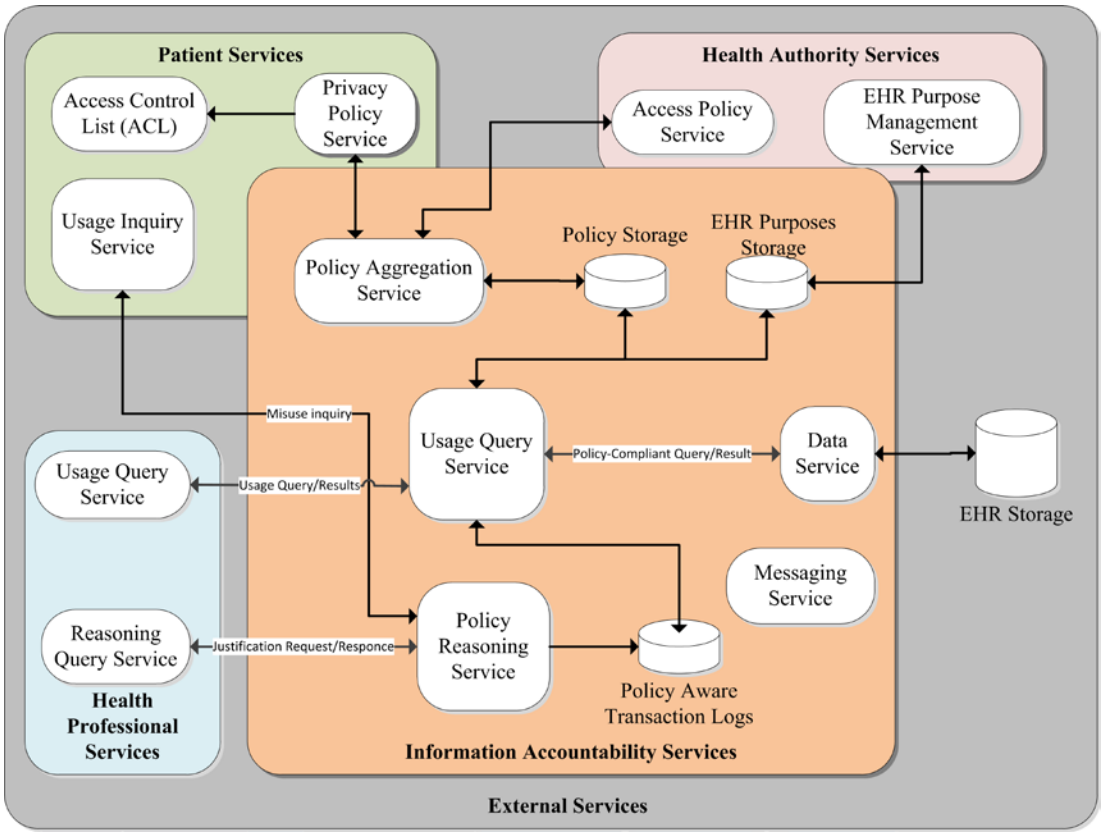


Figure 6.1 Schematic AeH system architecture (Gajanayake, Iannella, & Sahama, 2012)

A schematic architecture is shown in Figure 6.1. The architecture is divided into two categories of services; *external services* and *internal services* and has three types of users; patients (*P*), a healthcare authority (*HA*) and healthcare professionals (*HCP*).

Internal services consist of a *policy aggregation service*, the *information accountability services*, a *messaging service*, a *data service*, *policy storage* and the EHR *Purpose storage*. External services of the architecture include *patient services*, *health authority services*, *health professional services* and the external *EHR storage*. Detailed descriptions of these services are given in the following sections.

6.3.2 Internal Services

Information accountability services consists of *policy storage* (PS_{IAS}), *policy aware transaction logs* ($PATL_{IAS}$) and policy services containing a *usage query service* (UQS_{IAS}) and a *policy reasoning service* (PRS_{IAS}). PS_{IAS} stores the policies it receives from the *policy aggregator service*. UQS_{IAS} processes the usage queries it receives from health professional services requesting access to EHR data. Once the policy service receives an *inquiry query* from patient services PRS_{IAS} send a request

to the health professional service requesting a *reasoning query* for a particular information usage instance. The reasoning queries are processed with the use of $PATL_{IAS}$ which contains all past transactions of the system.

Other internal services include a *policy aggregator service* (PAS_{IS}) which amalgamates the policies from PPS_P and APS_{HA} as discussed in section 5.4.4 in chapter five, a *data service* (DS_{IS}) which is the only component with access to the EHR storage, a *messaging service* (MS_{IS}) that sends out the relevant messages to other services and an *EHR purposes storage* (EPS_{IS}) which consists of the intended purposed of each of the data types in the *EHR*. The EPS_{IS} is managed by *HA.*

6.3.3 External Services

External services are used by the end users to give inputs to the internal services and receive results from them. External services consist of patient services, health authority services, health professional services and the EHR storage.

Patient services are used by a patient to manage their EHR. The patient services consist of an *access control service* (ACS_P), *privacy policy service* (PPS_P), *messaging service* (MS_P) and a *usage inquiry service* (UIS_P). A patient maintains an access control list (ACL) with the use of ACS_P. The patients set their privacy policies using *PPS* and assign sensitivity levels for trusted health professionals in the ACL. These policies are then amalgamated by the *policy aggregation service* (PAS_{IS}) with the policies of the health authority and stored in PS_{IAF}. Patients receive notifications and can send messages to HCPs through the MS_P from the internal services. Notifications include regular updates on the EHR, notifications of information access by HCPs, warnings of potential information misuse and messages from HCPs. All messages need to go through the internal services for them to be recorded in the Transaction logs.

Health authority services are used by a central health authority to manage access settings for health professionals. Health authority services consists of a *role based access control service* ($RBACS_{HA}$), an *EHR purpose management service* ($EPMS_{HA}$) and *access policy service* (APS_{HA}). The HA set minimum access levels for HCPs using APS_{HA} together with $RBACS_{HA}$. These policies are combined with the patient's privacy policies according to the access control protocol in chapter five. HA uses $EPMS_{HA}$ to manage the EHR purposes in $EPS_{IS.}$

Healthcare professional services are used by health professionals to access patient EHR information. HCPs are able to perform actions such as read, write and update. HPs are also able to initiate information sharing requests in order to share patient health information with other HPs to make informed decisions. Health professional services include a *usage query service* (UQS_{HCP}), a *reasoning query service* (RQS_{HCP}) and a *messaging service* (MS_{HCP}). HCPs can lodge usage queries using UQS_{HCP} requesting access to EHR information. These queries contain purposes for which information is required. The queries are processed by the UQS_{IAS} and if they are policy compliant access is granted. If the usage queries are not policy compliant a warning notification is sent to the requester at which point he can either comply with the warning or disregard it. If the warning is disregarded and the data is accessed by the HCP, a message is sent by the MS_{IS} to MS_{P} notifying the patient of potential information misuse. At this point the patient may initiate a usage inquiry using UIS_P. As a result PRS_{IAS} sends a request to RQS_{HCP}. The HP then has to send a justification of the use of information in the form of a reasoning query through the RQS_{HCP}. The justification is processed by the PRS_{IAS}. If the provided justification is valid the incident is resolved. If not, further action (such as legal action) would be taken which we would not discuss in this thesis. PRS_{IAS} should have the capability to deduce whether a provided justification is valid. This process of inquiries and resulting justifications enables the system to detect intentional misuse of data by users.

6.3.4 Information accountability service

The IA service is the core of the IAF which processes user requests. It contains a policy aggregator service (PAS_{IAS}), a policy storage (PS_{IAS}), a usage query service (UQS_{IAS}), a policy aware transaction logs ($PATL_{IAS}$), a policy reasoning service (PRS_{IAS}), a messaging service (MS_{IAS}), a data service (DS_{IAS}) and an EHR purposes storage (EPS_{IAS}).

PAS_{IAS} amalgamates the policies set through PPS_{P} and APS_{HA} in such a way that the patient's privacy requirements are met and the health authorities' policies also be satisfied. The policies are stored in PS_{IAF}. UQS_{IAS} processes the usage queries it receives from HCPs requesting access to EHR data. The queries are processed using PS_{IAS} and EPS_{IAS} which consists of the intended purposed of each of the data types in the EHR and is managed by HA. All transactions are stores as policy-aware

transaction logs in $PATL_{IAS}$. Once an inquiry query is received from patient services, PRS_{IAS} sends a request to the health professional service requesting a reasoning query for a particular information usage instance. The resulting justifications or reasoning queries are processed with the use of $PATL_{IAS}$. DS_{IAS} retrieves data from EHR storage. This is the only component with access to the EHR data. MS_{IAS} sends out messages to external services.

6.4 IA PROTOCOLS

The functionality of the IA services is depicted in a Specification Description Language (SDL) diagram in Figure 6.2.

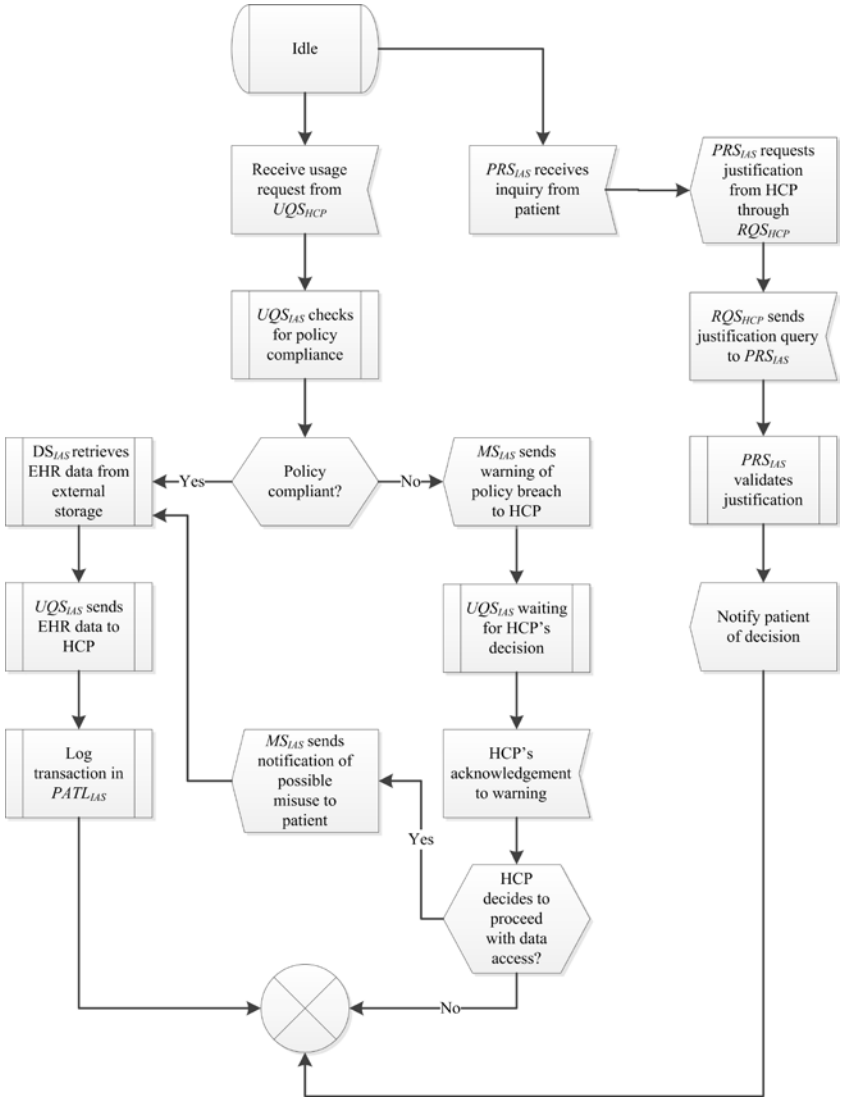


Figure 6.2. SDL diagram for the IA services

A message sequence of the IA service in the event of possible information misuse by an HCP is shown below in Figure 6.3.

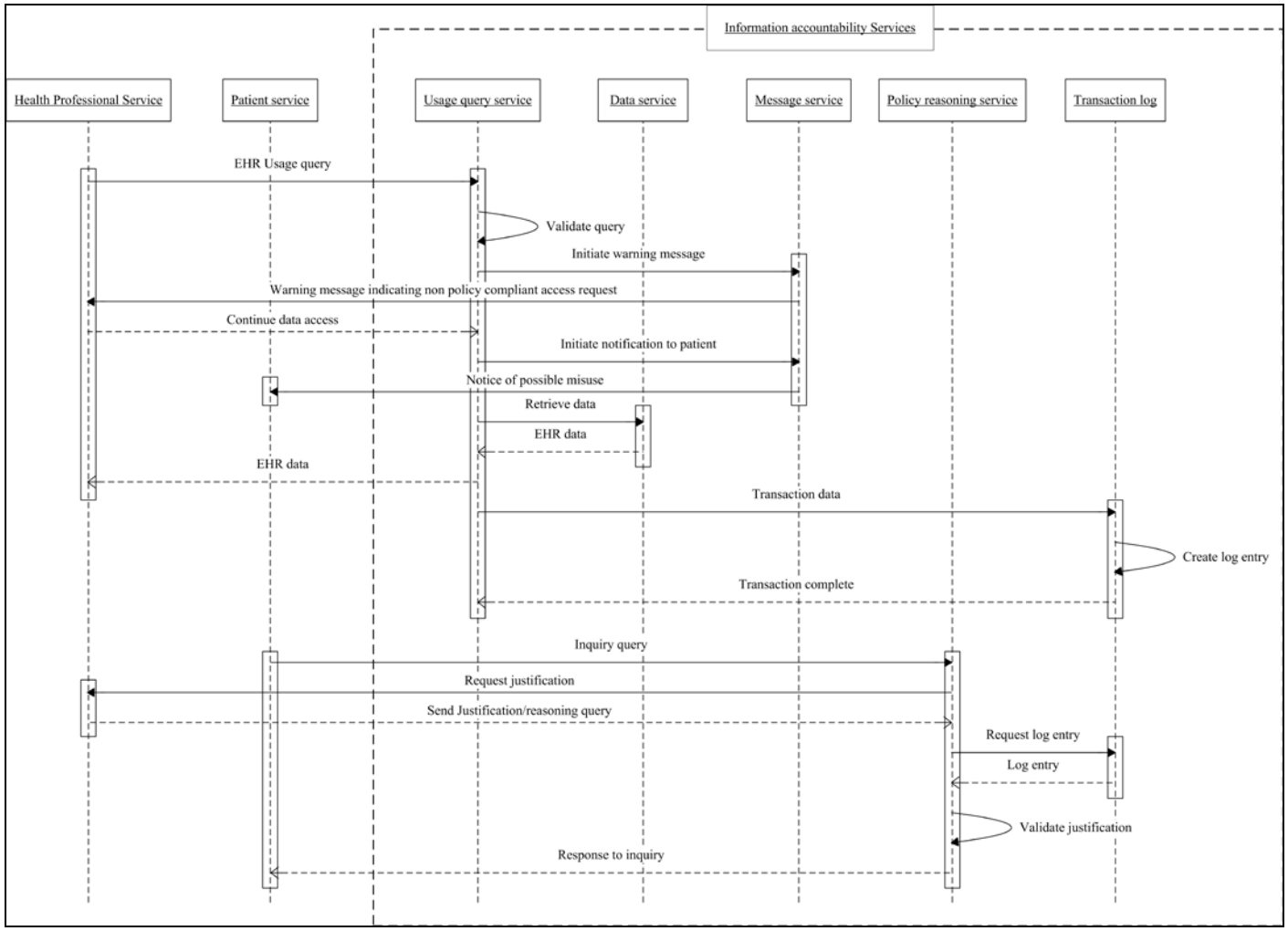


Figure 6.3. Message sequence of IA service in the event of a possible misuse of information

6.5 FEASIBILITY

In this section we present solutions for the policy related aspects mentioned throughout the thesis. We use an open standard policy language, namely; the Open Digital Rights Language (ODRL) to show how the policies discussed in chapter five are expressed in AeH systems. The prototype presented in chapter five was used to implement an extension to the ODRL core model to enable a transaction logging capability. We give an account as to how the transaction logs and the policies are formulated and expressed in ODRL.

6.5.1 Overview

The initial reviews done on the approaches to information accountability in chapter two revealed that policy formulation and representation are key aspects of accountable-systems. For this reason, the main focus of this chapter will be policy representation in the IAF. The Semantic reasoning capabilities of the IAF are discussed but will not be addressed in terms of a technology solution. Rather, a possible implementation approach is discussed with the use of Semantic Web technologies. Current research in the Linked-Data arena shows that these capabilities are not far away from being readily available to end users (Berners-Lee, Hendler, & Lassila, 2001).

6.5.2 Digital rights management

The IAF is policy driven. The proper representation of the policies is thus vital. In this section we will give an account of the technical aspects to policy representation. The data elements in the EHR can be considered as digital assets and the policies can be set on those assets to manage their usage. As a technical solution for this, we look to technologies in the digital rights management (DRM) arena. Apart from their applications in copyright protection of media files, etc on the Internet, DRM technologies are becoming a prominent resource in protecting private information of individuals (Feigenbaum, Freedman, Sander, & Shostack, 2002). DRM has many similarities to the traditional access control model but differs in that they require information to remain protected even after access is granted to authorised users. DRM thus deals with controlling the usage of an information resource by authorised users, i.e. enforcing usage policies. Each piece of information is protected by a usage license created by the digital rights holder. DRM can benefit

eHealth technologies by providing a means to manage the use of EHRs. Although DRM mainly deals with policy enforcement as previously mentioned, our approach is focused on the use of the open standard policy language for the expression of policies that can be used for accountability rather than their enforcement.

6.5.3 Open Digital Rights Language

The Open Digital Rights Language (ODRL) (Iannella, 2002) is a Rights Expression Language (REL) based on XML and provides a syntax and semantics to express policies related to digital assets. The ODRL core model is formally specified in UML and the language syntax is defined XML schema. The ODRL Requirements document contains requirements for the language that have been gathered since ODRL Version 1.1 has been released. An ODRL Vocabulary document specify the potential terms (vocabulary) used by the Core Model for policy expression needs across communities. In early 2009, ODRL Version 2.0 was released. The core model of ODRL V2 is shown in Figure 6.4.

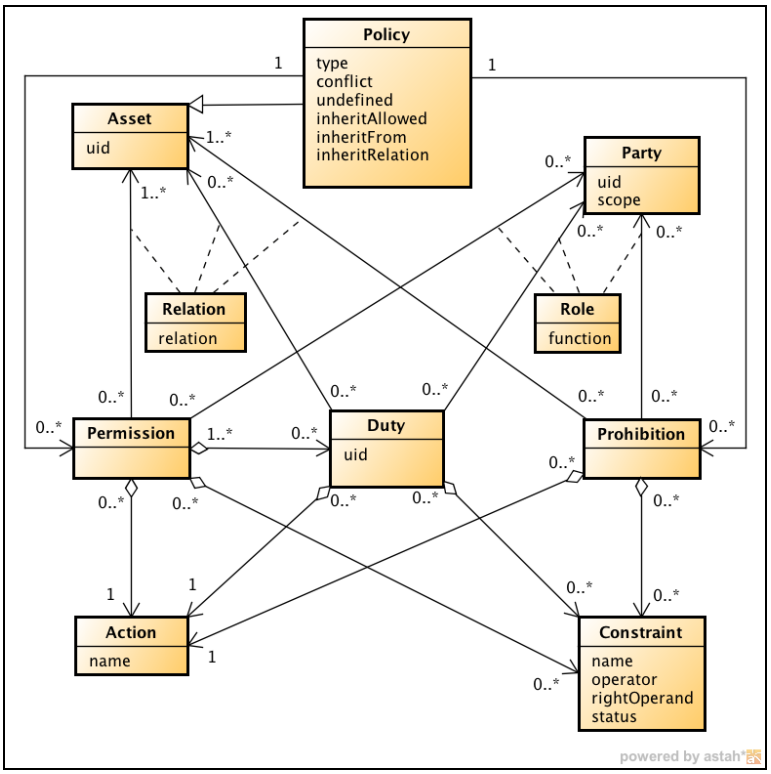


Figure 6.4 ODRL Version 2 Core Model (ODRL Initiative, 2012)

The ODRL Version 2.0 is a major update from Version 1.1 and provides is endorsed by the W3C ODRL Working Group as appropriate for widespread

deployment and use by the wide community. ODRL has been endorsed by a number of prominent organisations including Nokia and Open Mobile Alliance (OMA).

We have chosen ODRL as the policy language for AeH systems because it is independent of implementation constraints and it is capable of expressing a wide range of policy-based information. The semantics of ODRL falls neatly in line with the protocols we have developed for the policy formulation and representation. For example in the AeH system architecture, we deal with policy assigners and assignees, permissions and prohibitions, usage constraints, purposes and actions. ODRL supports all of these aspects.

6.5.4 An extension to the Core Model

It was previously established that transaction logs in an accountability system need to be policy aware. To make this feasible, we have extended the current model of ODRL.

In accountability systems, policy violations and *after-the-fact* accountability are key aspects. In order to identify and redress violations, a policy-aware transaction log is maintained. The current ODRL core model is incapable of supporting audit logs. We present an extension to the current ODRL model to capture the required semantics necessary for policy-aware transaction logs and later for policy reasoning. We have extended the core model to be able to store policy-aware transaction logs using ODRL. The logs have to capture data such as what data was accessed, the intended purpose of the access or usage, the underlying policy for access and usage. Furthermore they need to capture the identity of the data consumer, nature of transaction, time of transaction, location of the transaction (e.g. through a doctor's local EMR), the status of the transaction (valid or invalid). The logs are *read only* and *immutable*. We assume that the transaction logs are encrypted and secure in order to protect their integrity.

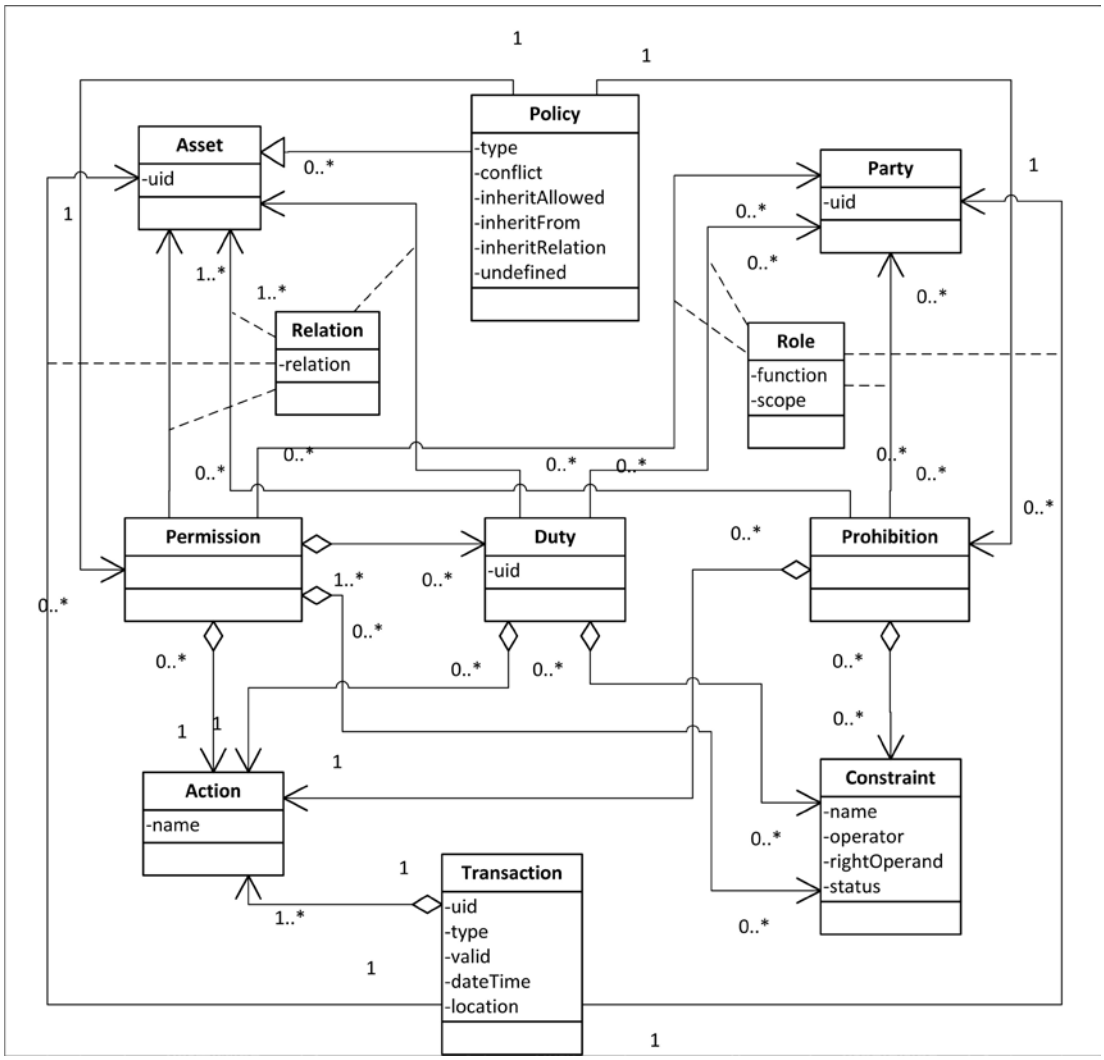


Figure 6.5 Extended ODRL Core model

A new entity '*Transaction*' is introduced to the ODRL core model (see Figure 8.3). Together with the current ODRL semantics, additional semantics are introduced to the *Transaction* entity.

Semantics of "Transaction"

The *Transaction* entity deals with information related to past transactions and contains the following attributes:

uid: the unique identification of the *Transaction* entity

valid: indicates the transaction to be a valid or invalid transaction. This will identify the transaction as potential misuse of data or violation of a related policy. Allowed values are *True* or *False.*

type: The transactions may be of the following types. This list is not exhaustive.

generalUse – authorised users using assets

sharedUse – usage resulting from sharing requests sent by authorised users

dateTime: indicates the date and time of the transaction

location: the EMR/device/location used to access the data

The Transaction entity refers to *Action*, *Asset* and *Party* entities to identify and store the relevant data of a transaction. A transaction is accompanied by its corresponding usage policy. Transaction entity captures the actions performed by the user on a retrieved asset. In an auditing instance, a single transaction log contains sufficient information to make a comparison with a violated policy without having to retrieve the policy itself. This is useful in events where policies may evolve with time.

A transaction may contain more than one action on an asset retrieved by a user. One transaction may only have one asset and one or more actions performed on that asset by one party. A user can perform many actions on a set of data retrieved through one access request. This is different to the current ODRL models' semantics.

6.5.5 ODRL Policies

Consider the healthcare scenario presented in chapter two. Patient X allows Dr. S to access his EHR but restricts her from accessing his sexual health details and mental health details. Below is an ODRL V2 XML instance of this policy.

```
<o:policy xmlns:o= "http://w3.org/ns/odrl/2" xmlns:eh="urn:ehealth.gov" type="
http://w3.org/ns/odrl/2/privacy" uid="policy-use-ehr" conflict="o:prohibit">
  <o:permission>
    <o:asset uid="urn:ehr:Patient X" relation="o:target"/>
    <o:party uid="urn:patient:Patient X" role="o:assigner"/>
    <o:party uid="urn:healthPro:dermatHealth:Dr. S" role="o:assignee"/>
    <o:action name="o:read"/>
  </o:permission>
  <o:prohibition>
    <o:asset uid="urn:ehr:Patient X:sexualHealthCare" relation="o:target"/>
    <o:asset uid="urn:ehr:Patient X:mentalHealthCare" relation="o:target"/>
    <o:party uid="urn:patient:Patient X" role="o:assigner"/>
    <o:party uid="urn:healthPro:dermatHealth:Dr. S" role="o:assignee"/>
    <o:action name="o:read"/>
  </o:prohibition>
</o:policy>
```

The conflict attribute of the policy above is set to "*prohibit*" indicating that prohibitions take precedence in the policy. The health authority can set an access policy for Dr. S which is given below.

```
<o:policy xmlns:o= "http://w3.org/ns/odrl/2" xmlns:eh= "urn:ehealth.gov" type="
http://w3.org/ns/odrl/2/agreement" uid="policy-use-ehr">
  <o:permission>
    <o:asset uid="urn:ehr:Patient X:dermatHealthCare" relation="o:target"/>
    <o:asset uid="urn:ehr:Patient X:sexualHealthCare" relation="o:target"/>
    <o:party uid="urn:health:authority" role="o:assigner"/>
    <o:party uid="urn:healthPro:dermatHealth:Dr. S" role="o:assignee"/>
    <o:action name="o:read"/>
  </o:permission>
</o:policy>
```

The health authority is responsible for setting default access policies for healthcare roles, in this case for the role of a dermatologist. In the policy above HA gives Dr. S the permission to access Patient X's dermatology details and sexual health details. Note here that Patient X's settings prohibit Dr. S from accessing his sexual health details. But we assume a hypothetical scenario where a relationship between skin conditions and STDs exist, and every dermatologist should have access to the patient's sexual health details. The health authority is aware of this fact and allows all dermatologists access to patients sexual health details. According to the access control protocol in section 3, the settings by the health authority always prevail over patient settings. The final policy will be a combination of the two policies and hence the requirement for PAS_{IS} in the IAF. The amalgamated policy for Dr. S is given below.

```
<o:policy xmlns:o= " http://w3.org/ns/odrl/2" xmlns:eh="urn:ehealth.gov" type="
http://w3.org/ns/odrl/2/privacy" uid="policy-use-ehr" conflict="o:prohibit">
  <o:permission>
    <o:asset uid="urn:ehr:Patient X" relation="o:target"/>
    <o:party uid="urn:patient:Patient X" role="o:assigner"/>
    <o:party uid="urn:healthPro:dermatHealth:Dr. S" role="o:assignee"/>
    <o:action name="o:read"/>
  </o:permission>
  <o:prohibition>
    <o:asset uid="urn:ehr:Patient X:mentalHealthCare" relation="o:target"/>
    <o:party uid="urn:patient:Patient X" role="o:assigner"/>
    <o:party uid="urn:healthPro:dermatHealth:Dr. S" role="o:assignee"/>
    <o:action name="o:read"/>
  </o:prohibition>
</o:policy>
```

This final policy is stored in PS_{IAS} and is used by other services. Updates are done to the policies in PS_{IAS} accordingly. HCPs in already in the ACL can lodge usage requests to the EHR system.

Information sharing

Information sharing is an important aspect of healthcare and is facilitated in the IAF. HCPs who are already in the ACL can initiate sharing requests.

```
<o:policy xmlns:o="http://odrl.net/2.0" xmlns:eh="urn:ehealth.gov" type="
http://w3.org/ns/odrl/2/request" uid="policy-share-ehr">
  <o:permission>
    <o:asset uid="urn:ehr:Patient X:dermatHealthCare" relation="o:target"/>
    <o:asset uid="urn:ehr:Patient X:sexualHealthCare" relation="o:target"/>
    <o:party uid="urn:healthPro:dermatHealth:Dr. S" role="o:assigner"/>
    <o:action name="o:share"/>
    <o:constraint name="o:purpose" operator="o:eq"
rightOperand="eh:dermatHealthCare">
    <o:constraint name="o:recipient" operator="o:eq"
rightOperand="urn:healthPro:sexualHealth:Dr. B">
  </o:permission>
</o:policy>
```

In the policy above Dr. S initiates a request to share Patient X's dermatology details with Dr. B. Dr. B accepts this request by lodging the following access request to read Patient X's dermatology details. Requests resulting from sharing requests are allowed (holding to general access policies) since the initial request was from a HCP already in the ACL.

```
<o:policy xmlns:o= " http://w3.org/ns/odrl/2" xmlns:eh="urn:ehealth.gov" type="
http://w3.org/ns/odrl/2/request" uid="policy-use-ehr">
  <o:permission>
    <o:asset uid="urn:ehr:Patient X:dermatHealthCare" relation="o:target"/>
    <o:asset uid="urn:ehr:Patient X:sexualHealthCare" relation="o:target"/>
    <o:party uid="urn:healthPro:sexualHealth:Dr. B" role="o:assignee"/>
    <o:action name="o:sexualHealthcare/investigate"/>
    <o:constraint name="o:purpose" operator="o:eq"
rightOperand="eh:dermatHealthCare">
  </o:permission>
</o:policy>
```

In the usage request above, Dr. B requests Patient X's dermatology and sexual health information from the EHR system. The purpose for Dr. B's data access is an investigation related to Patient X's sexual health.

Audit logs

Below is an ODRL transaction log is a result of a successful access request by Dr. S to access Patient X's dermatology details for the purpose of *dermatHealthCare*. The audit log contains the existing access policy for Dr. S.

```
<o:policy xmlns:o= " http://odrlextension.org/ns/odrlx/2x" xmlns:eh="urn:ehealth.gov"
type=" http://odrlextension.org/ns/odrlx/2x/privacy" uid="policy-use-ehr"
conflict="o:prohibit">
  <o:permission>
    <o:asset uid="urn:ehr:Patient X" relation="o:target"/>
    <o:party uid="urn:patient:Patient X" role="o:assigner"/>
    <o:party uid="urn:healthPro:dermatHealth:Dr. S" role="o:assignee"/>
    <o:action name="oe:read"/>
    <o:constraint name="o:purpose" operator="o:eq"
rightOperand="eh:dematHealthCare"/>
  </o:permission>
  <o:prohibition>
    <o:asset uid="urn:ehr:mentalHealthCarePatient X" relation="o:target"/>
    <o:party uid="urn:patient:Patient X" role="o:assigner"/>
    <o:party uid="urn:healthPro:dermatHealth:Dr. S" role="o:assignee"/>
    <o:action name="o:read"/>
  </o:prohibition>
  <o:transaction uid = "transaction-use-ehr" valid = "o:true" type = "o:generalUse"
dateTime = "o:164001072012" location = "urn:emrlocation.org/Dr. S">
    <o:asset uid="urn:ehr:Patient X" relation="o:target"/>
    <o:party uid="urn:healthPro:dermatHealth:Dr. S" role="o:user"/>
    <o:action name="o:dermatHealthCare/patientVisit"/>
  </o:transaction>
</o:policy>
```

The policies at the time of action are attached to every transaction log. This enables an efficient auditing process not having to retrieve past policies that may have changed after the actions have occurred.

Although policies can be successfully represented and managed using ODRL as shown above, in order for the reasoning capability of the IAF to be technologically feasible, we have to consider ODRL in the Semantic Web domain. Next we will present a technology overview of how we can use ODRL in conjunction with semantic web technologies and how we can attain the reasoning capabilities proposed in the IAF.

6.5.6 Implementation on the Semantic Web

Although it is proposed as a semantic reasoning process, the reasoning capabilities of the IAF are not technically validated in this thesis. However, we give an overview of the semantic technologies that can be used to address this capability as a technical solution. The technologies in question are Semantic Web technologies.

The Web is gradually transforming to what is called “the Semantic Web” where the traditional Syntactic Web is leveraged towards a distributed knowledge repository. The semantic web is based on the Resource Description Framework (RDF) (Lassila & Swick, 1999) for metadata semantics and the Web Ontology Language (OWL) (McGuinness & van Harmelen, 2004) for web ontologies. These technologies enable the development of Web based information systems that are capable of automated reasoning, impossible with the syntactic web. They open new avenues for eHealth systems.

ODRL is a solution to move DRM to the Internet. But in order to enforce the semantics of the policies in conjunction with ODRL, a corresponding ontology is required. The present ontology (Iannella, 2012) need to be extended to capture the semantics of the ODRL extension discussed earlier. The ontology for the policies can be represented using OWL. Such an ontology allow us to achieve the reasoning capabilities proposed in the IAF.

EPS_{IS} contains an ontology representing the relationships between the EHR data themselves and eHR data and the intended purposes. This ontology together with a comprehensive medical ontology enables us to infer facts otherwise would not be available. For example, the presence of the fact that Patient X has a particular allergy in the EPS_{IS} can lead to the inference of the fact that a particular medication has the tendency to be harmful to Patient X. This fact would not have been available to the EHR system without a specific external input specifying this or if Patient X has had an illness which is usually treated by this particular medication. The inferences are updated with new data and facts available to EPS_{IS}. The policies in PS_{IAS} are stored in RDF with vocabularies from the ODRL ontology. The queries made by UIS_P and PRS_{IAS} are made in a RDF query language like SPARQL (Prud'hommeaux & Seaborne, 2008). Data stored in $PATL_{IAS}$ is also in RDF allowing mining to be done using SPARQL. Together with these services and a policy aware reasoner, PRS_{IAF} allow us (with a suitable natural language translation middleware) to process queries such as “*Why did Dr. S read my sexual health details?*” by Patient X. Similarly, Dr. S will be able to justify why she read Patient X’s sexual health details. The validity of the justification is determined after mining the $PATL_{IAS}$ and PS_{IAS}. Provided justification holds if the facts confirm with the available knowledge. Note here that as mentioned above, the patient can only lodge an inquiry query if

there has been a possible misuse of data i.e. some underlying policy has been violated by the user. The justification is on why the user has done so. The ontologies defined enable us to infer facts that validate the justification. For example, in an emergency situation the treating health professional will access all necessary information from the eHR regardless of the privacy and access policies. This will be recorded in $PATL_{IAS}$. For any inquiry made by the patient to clarify data usage related to this episode of care, the fact that the incident was considered and recorded as an emergency would validate the justifications given by the health professionals.

6.6 A PROTOTYPE FOR THE ODRL POLICIES

We extended the previously mentioned Web prototype as a test vehicle to demonstrate the use of ODRL. This prototype does not demonstrate the Semantic Web technological model described in the previous section. Policy setting and computation is done according to the model described in chapter five. All usage requests and communications with the system by end users are logged using the extended ODRL model. The system determines possible inappropriate use of data and the patients are capable of lodging inquiries about possible misuse of data.

The purpose of the prototype was to demonstrate the protocols and to validate the designed technical architecture in terms of the policy management and to validate the ODRL extension. Further work is required before the Semantic reasoning capabilities of the IAF can be integrated into a working solution.

6.7 PROTOCOL SIMULATION

Model checking is used as a technique of automatically debugging complex reactive systems (Vaandrager, 2011). The system specifications are expressed as logic formulas and efficient symbolic algorithms are used to traverse the model defined by the system and check if the specification holds thus allowing the analysis of models that capture the dynamic behaviour of systems. In this section we use a model checking approach to validate the protocols of the architecture and show that it behaves as intended. We use the model checking tool UPPAAL for this task.

6.7.1 Overview of UPPAAL

UPPAAL is a toolbox for verification of real-time systems developed as a result of joint efforts by the Department of Information Technology at Uppsala

University in Sweden and the Department of Computer Science at Aalborg University in Denmark (Behrmann, David, & Larsen, 2004; Vaandrager, 2011). Using UPPAAL, it is possible to verify systems that can be modelled as a collection of interacting communicating timed automata (Alur & Dill, 1994). UPPAAL has been successfully used in case studies ranging from communication protocols to multimedia applications (Behrmann, et al., 2004) and is available for free academic use and for licensed commercial use.

The UPPAAL graphical user interface consists of three main parts: the *system editor* that is used to construct models, the *simulator* that is used to simulate the behaviour, and the *verifier* that is used to analyse the behaviour of the model. A model of a system can be expressed using a graphical notation with global and local variables, clocks and synchronisation channels. Synchronisation channels consists of output channels, represented as *VarName!*, and input channels, represented as *VarName?*, and are used to synchronise two automata in the system, where *VarName* is the name of the synchronising variable. Once *VarName!* is invoked, *VarName?* is triggered.

The system model can be run automatically or selected transactions can be manually triggered. The behaviour of the system can be checked via a message sequence chart corresponding to the transactions generated by UPPAAL from within the simulator. Further analysis can be done using the verifier where specific characteristics of the system can be checked using queries. These queries can be used to check whether a specific property of the system holds or not. UPPAAL uses *Brute-Force* to do exhaustive searches to validate these queries.

6.7.2 UPPAAL Model for the Architecture

The system model consists of eight automata that represent each interacting agent: the patient service, the healthcare professional service, the usage query service, the reasoning query service, the policy store, transaction logs, the data service and the message service. We present the main component of the model here and the simulation results in the form of message sequence charts. The rest of the automata are included in Appendix F.

We assume that usage policies are already created and stored in the policy store. Therefore the healthcare authority is not modelled into the system in this

instance. The relevant services for information access and usage and the resulting accountability services are modelled. The usage query service receives usage requests from healthcare professionals and processes the requests. Figure 6.6 shows the UPPAAL model for the usage query service.

The healthcare professional service handles operations such as usage requests and receive and response of messages from the EHR system. Figure F.1 in Appendix F shows the UPPAAL model for the healthcare professional service. Although in the AeH model the reasoning process involves the healthcare authority, we have modelled it as an automated service as proposed in section 6.5.6. The UPPAAL model for the policy reasoning service is shown in Figure F.2 in Appendix F.

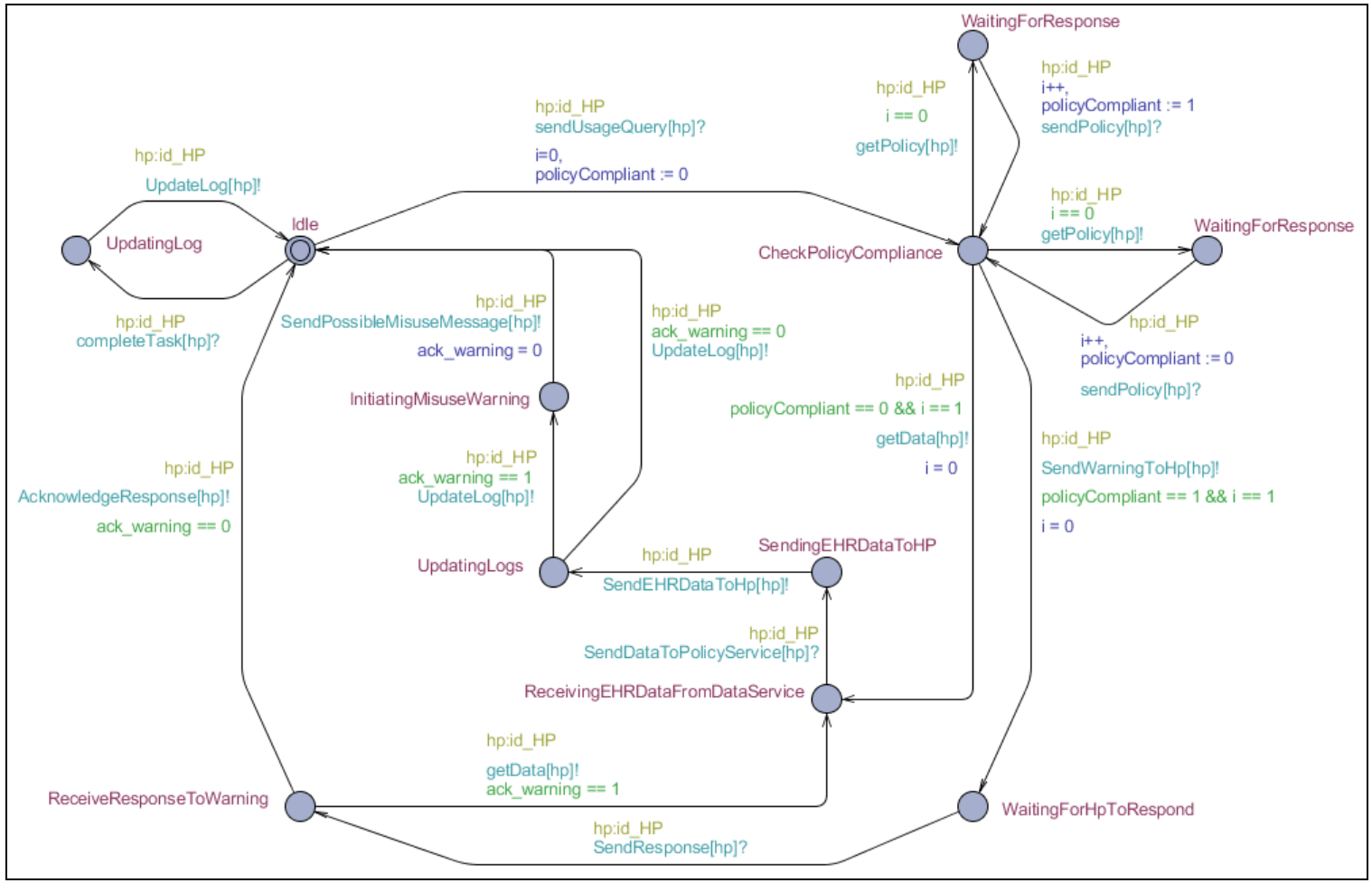


Figure 6.6 Usage Query Service UPPAAL model

6.7.3 Simulations

Simulations begin by assuming that the relevant usage policies are available in the policy store (EHR purposes and policies are regarded as one combined entity). A healthcare professional initiates a usage query through the *Healthcare Professional Service* that is sent to the *Usage Query Service*. The *Usage Query Service* validates the query by checking the HCPs usage policy by retrieving the policies from the *Policy Service*. The result is modelled as a random update of a variable. If the usage request is policy compliant, the requested data is retrieved from the EHR data store and forwarded to the HCP. The event is logged by the *Transaction Logging Service*. If the request is not policy compliant, the HCP is issued with a warning message through the *Message Service*, which the HCP has to acknowledge before continuing. The HCP has the option to either terminate the usage request or continue with the information access. If the prior occurs, the event terminates here and the event is logged by the *Transaction Logging Service*. If the later occurs, the data from the EHR will be retrieved via the *Data Service* and passed on to the HCP and a notification is sent to the *Patient Service* by the *Message Service* informing of a possible misuse of information by the relevant HCP. The information access is logged by the *Transaction Logging Service*. The patient is given the option to inquire about this event in the form of an inquiry query sent to the HCP. The HCP is required to send a justification to this inquiry query, which is validated by the *Policy Reasoning Service*. The justifications are validated by retrieving the transaction logs contained in the Policy-Aware Transaction Logs via the *Transaction Logging Service*. The outcome (whether policy compliant or not) is notified to the patient and the HCP. The procedure for redress after this process is outside of the technical architecture of the IAF. There is a possibility of continuous misuse of information by HCPs. To address this, a property was implemented where if an HCP misuses a patient's information, that HCP cannot access further details of that specific patient. The only action that HCP can perform is justification of the misuse in responding to the patients query.

Several possible scenarios were simulated and the model behaved as intended. The model is capable of handling data access by multiple HCPs. Unique transaction threads are used to handle information access requires by different HCPs.

After the simulations were performed, the *Verifier* of the UPPAAL tool was used to check whether specific states are reached in the model that must be reached if the protocols work as intended. The result of the *Verifier* is either "*Property is satisfied*" or "*Property is not satisfied*".

First, the model was tested for deadlocks by running the following query in the *Verifier*.

A[] not deadlock

The result indicated that the property is satisfied. After establishing the model was deadlock free, multiple simulations were observed to identify possible *livelocks*. None were found. Further queries were then tested to verify that the model is working as intended. For example, the fact that a healthcare professional cannot access information if a misuse has occurred can be tested using the following query.

E<> (HealthProfessional(0).RequestingEHRData &&
HealthProfessional(0).misuseEvent == true)

The query asks if a state exists where the *Healthcare Professional Service* can be in the state where it request EHR Data whilst there has been a misuse of information by the same HCP previously that has not being resolved. The result of the Verifier indicated that "*Property is not satisfied*", which indicated that our goal is achieved. Similarly patient notifications at the point of misuse can be checked using the following query.

E<> (HealthProfessional(0).misuseEvent == true &&
HPQuery.InitiatingMisuseWarning)

The *Verifier* indicated the "*Property is satisfied*", indicating that when an HCP misuses information a warning is sent to the patient by the *Usage Query Service (HPQuery* is the identifier given to the instance of the *Usage Query Service* in the UPPAAL model). Also, the requirement that an HCP has to give a justification for a possible misuse of data can be verified through the following query.

E<> (PatientX.RequestingJustification &&
HealthProfessional(0).JustifyingAction)

The result returned by the *Verifier* was "*Property is satisfied*", as expected. A MSC of from an UPPAAL simulations is given in Figure 6.7.

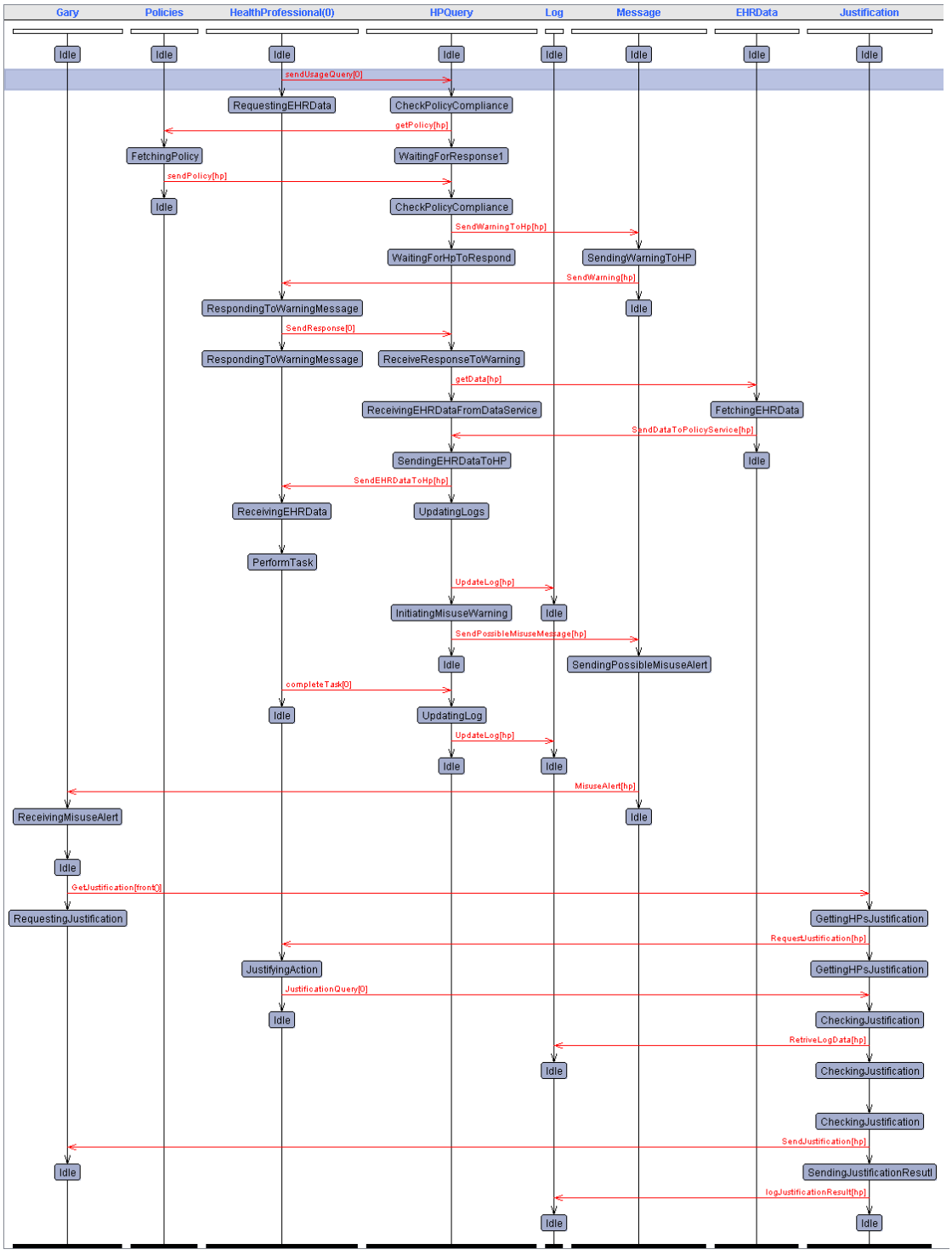


Figure 6.7 Simulation results for a scenario of possible misuse of information by an HCP

6.8 DISCUSSION AND CONCLUSION

In this chapter, we have presented a technical architecture for the information accountability framework (IAF). In our model we used ODRL as the policy language and discussed how we can represent the different privacy and access policies in the IAF. An extension to the current ODRL core model was also presented to facilitate for policy-aware transaction logs, which are essential for accountability systems. The architecture presented here focus on the internal communications of the system that are related to the IA principles presented in chapter two. We assumed that all communication channels are secure. The use of ODRL for policy representation was validated using an extension of the Web prototype used in chapter five. The entire architecture was modelled using UPPAAL and the behaviour was simulated as a validation.

Policy reasoning is a characteristic of AeH systems. Although this process can be managed by an *accountability advocate*, an automated procedure was proposed. Currently the only technologies that provide such capabilities are Semantic Web technologies. We discussed how we can use these technologies such as OWL ontologies and RDF to develop the presented architecture. It is clear that developing a comprehensive EHR system with an IAF is an immense undertaking. But with the level of technology currently at the disposal of developers it is without a doubt feasible task. Semantic Web based policy management has been studied by many and some attractive solutions have been proposed (Kagal, Finin, & Anupam, 2003; Kagal, Finin, & Joshi, 2003; Tonti et al., 2003). However, we chose ODRL as the policy language for our model to give us the flexibility needed to extend the existing model to suit the capabilities introduced in our model.

The architecture presented in this chapter enables transparent use of health information and to detect when possible misuse of information occurs. It is the patients right to pursue the violators for compensation or other remedies. The patient may seek assistance from the authorities responsible for managing the EHR to react to such situations. The patient may choose to ignore minor incidents which he or she sees are insignificant. But the patient always has the capability to inquire past incidents whenever a negative effect occurs which may be linked to EHR data misuse by health professionals. Further to this model, a medical practitioner's trust level can be determined with the use of techniques such as those of Alhaqbani and

Fidge (2009), Salim and Dulleck et al. (2011) and Salim and Reid et al. (2011). Continuous misuse of information in a system as this can be reduced by introducing an appropriate threshold for the trust level and preventive access to individuals when the threshold is exceeded.

In eHealth, accountability systems will enable the use of health information in a more free but controlled manner. This will allow health professionals to access relevant information at any point without the restrictions currently present in eHealth solutions. We believe that the presence of the IAF will increase the confidence level of the patients towards eHealth systems and would result in eHealth systems being better adopted. Barriers still exist in our venture towards building a working system with the capabilities introduced. Building a comprehensive EHR system is not our goal. Our goal is to show that with IA capabilities the current state of eHealth systems can be improved to a more open and trusted healthcare oriented state from a security and privacy oriented state.

Part Three: Implementation Aspects

Chapter 7: The IAF in the Australian eHealth System: A Case Study

In this chapter, we present a case study of the IAF within the Australian eHealth system to show how each component of the presented IAF would fit within the constraints of the existing eHealth infrastructure. This chapter will serve as a proof of the applicability of the IAF within an existing eHealth system. The case study was carried out by focussing on the infrastructure, access policies, nature of the data, legislation, data flow, and cost (financial, labour, time) of implementation. The main focus of this chapter is towards the legal issues related to Accountable-eHealth systems in Australia.

7.1 INTRODUCTION

Australia's healthcare system is under considerable reform with the introduction of eHealth, an ICT enabled approach to providing safe, reliable and efficient healthcare for all Australians (EHealth, 2012). eHealth aims to centralise all health information from general practices, hospitals and specialist clinics across Australia and provide patients with a single Personally Controlled Electronic Health Record (PCEHR). It is accepted that the move from fragmented local medical records to centralised electronic health records will reduce costs and result in safer healthcare; however there are concerns over how this sensitive information can be properly managed to ensure patient privacy without hindering healthcare providers in administering time-critical care.

eHealth currently relies on preventive security measures such as access controls to provide information security. While this purely preventative approach may be appropriate in the business setting, it is accepted that such an approach is inadequate in the health setting as it can restrict healthcare providers from accessing information necessary for administering high-quality medical care (Feigenbaum, et al., 2012; Kagal & Abelson, 2010). In the previous chapters we presented and validated an after-the-fact Information Accountability Framework (IAF) that holds healthcare providers accountable for all uses of a patient's sensitive health information. By tracking all information transactions and automatically checking

those transactions against the relevant privacy policies, the IAF will deter breaches with penalties instead of trying to prevent all possible breaches with pre-emptive access controls. This approach is similar to law enforcement in the offline world (Feigenbaum, 2010) and is likely to achieve a much better balance between the need for information privacy and the need for information access.

There are significant benefits to be gained from the implementation of eHealth; the Australian Government could save not only $7.6 billion in healthcare costs by 2020, but also 5000 deaths, two million primary care and outpatient visits, 500,000 emergency department visits and 310,000 hospital visits each year (Peiris, 2012). While these benefits are well recognised, without participation in masse by Australian consumers and healthcare providers alike, who have been reluctant to involve themselves to date due to privacy and information access concerns, they will not be realised. It is thus imperative that adequate information security measures are implemented that increase stakeholder trust and confidence, encourage greater participation in the system and allow the Australian Government to fully capitalise on the financial benefits that eHealth has to offer.

This case study will investigate the current state of eHealth in Australia and critically analyse the PCEHR system to ascertain how effective current information security measures are at balancing the need for information privacy of consumers with the need for information access of healthcare professionals. Details of the IAF, its underlying concepts and its ability to rectify the downfalls of the current eHealth system will be discussed and an argument will be put forward as to why the IAF should be implemented. Finally, an explanation of how the IAF can be integrated with existing infrastructure and health information laws will be given.

7.2 eHEALTH IN AUSTRALIA

7.2.1 History

Australian eHealth emerged in the 1990s as a way of overcoming the ‘tyranny of distance’ for isolated health consumers and professionals (Jolly, 2011). Originally termed Telehealth, the concept aimed to alleviate some of the problems of remote and rural Australians in accessing medical care, through forms of technology such as facsimiles, videos and medical images (Lonie & Lyle, 1993). However it also promised many other benefits, such as:

Easing overall pressures within the health system, in particular rapidly escalating health costs;

- Keeping an ageing population out of institutions;
- Addressing some of the health inequity experienced by specific groups;
- Affording more flexibility in the delivery of services;
- Reducing unnecessary duplication of services, waiting times for patients and medical errors (Jolly, 2011).

Political parties were enthusiastic about the potential benefits for Australia's healthcare system, but from the very outset there were problems that threatened to derail the concept. In 1997 the Standing Committee on Family and Community Affairs (SCFCA) released a report, *Health on line*, which listed many substantial barriers in the development of a national eHealth system; privacy, support from the medical profession and national coordination were among the most prominent dilemmas. Politicians soon realised that the development and introduction of successful eHealth policies was a complex process (Jolly, 2011) that required a paradigm shift in medical systems and the attitudes of all participants.

Despite these challenges, the Australian Government continued to further the eHealth cause and established the National Health Information Management Advisory Council (NHIMAC) in 1999. NHIMAC was given a number of interrelated tasks intended to address barriers to eHealth identified in the SCFCA *Health on line* report (Jolly, 2011). One branch of NHIMAC, the National Electronic Health Records Taskforce, was tasked with evaluating the benefits and difficulties with adopting national electronic health records and proposing a plan for their introduction (Jolly, 2011). In 2000 the taskforce proposed the Health*Connect* project. The Better Medication Management System (BMMS) was one part of the Health*Connect* project that was trialled in 2001, 2002, 2003 and 2005 with limited success. It was found that policies were needed to encourage consumer and provider participation. Privacy issues also needed to be addressed; it was thought that the most popular consent model for consumers and providers was that providers assume consent unless otherwise notified (Jolly, 2011). Despite the findings of the BMMS trials and SCFCA *Health on line* report, many of the issues have still to be resolved.

In 2004, the Howard Government formed the National EHealth Transition Authority (NEHTA) to advance the eHealth agenda through the development of standards, clinical terminologies and patient and provider identifiers (Jolly, 2011, p24). Despite making progress in the collaboration of states and territories and raising awareness of eHealth on a national level, NEHTA was criticised for its 'cycle of criticism, defensiveness and isolation' (Boston Consulting Group, 2007). In Boston Consulting Group's (BCG) view:

> Where engagement did occur, it appears often to have been one way, with little acknowledgement of stakeholder requirements or suggestions, and little patience with their lack of pre-existing understanding. Two thirds of stakeholders said that NEHTA did not acknowledge or respond to their feedback when they had engaged (Boston Consulting Group, 2007).

Similarly:

> Two thirds of external stakeholders complained that NEHTA was not transparent enough. NEHTA has also delayed seeking important feedback from users until relatively late in the process, potentially missing out on practical advice on how to make solutions work in local contexts, or over-engineering aspects of them beyond what was required (Boston Consulting Group, 2007).

Criticisms of this nature have continued to surface. There have been suggestions that NEHTA should have been replaced by a more inclusive and powerful body that may have been better able to support eHealth initiatives, target investment funding, help identify solutions and coordination opportunities and encourage adoption of, and compliance with eHealth strategies (Deloitte, 2008). Despite its criticisms, when the Howard Government left office in 2007, NEHTA had laid the foundations on which the future of eHealth would be developed (Jolly, 2011).

Success elsewhere

Implementing a national eHealth system is an extremely complex and delicate task, requiring collaboration between all states and territories and the integration of localised hospital, general practice and specialist clinic infrastructure and software services. NEHTA CEO has likened the task to putting man on the moon; but it is achievable (Jolly, 2011). Around the world, numerous countries have attempted to

implement electronic health systems with varying degrees of success; Denmark is widely considered to be the shining example in this regard.

Denmark's national eHealth system is the result of four individual strategies implemented since 1996 that each aimed to provide value to patients and providers in the healthcare sector. Importantly, these strategies built on each other (Jolly, 2011). *Sundhed.dk*, the national eHealth portal launched in 2005, provides a single access point for consumers to book appointments with medical practitioners, order medications and renew prescriptions, review medication records, access health data and communicate with healthcare authorities. Healthcare providers can also use the portal to communicate about specific patients, access excerpts of records from hospitals and view other information such as laboratory results and data from electronic patient records (Jolly, 2011). Another initiative, MedCom, has allowed for a single form of communication between primary care physicians across 5000 health institutions and 50 vendor systems (Jolly, 2011). Denmark's national eHealth system is an undeniable success, with 98% of all primary care practices using these systems to make full use of the clinical functionality of electronic medical records (Jolly, 2011).

Australia's approach to a national eHealth system is not dissimilar to that of Denmark, with both systems revolving around a centralised health information network with a single point of access for consumers and healthcare professionals (Jolly, 2011). There are however some important differences between Denmark's system and Australia's. A number of laws are in place in the Danish system to protect patients' rights and patients are able to prevent the gathering or communication of their health information for use in their treatment. Denmark also has a much smaller, tech-savvy population of 5 million citizens compared with Australia's 22 million, and is geographically more condensed which has lessened interoperability challenges. The Danish medical profession has been engaged when determining the content of electronic health records and setting standards for data, and training has been provided to assist healthcare providers in the adoption process.

Perhaps the most important difference though is the high level of trust that Danes place in the federal government to firstly maintain a purely public health sector, and secondly to implement a national eHealth system within that sector (Jolly, 2011). This trust and confidence in governmental strategies which appears to have

underpinned the success of the Danish system is sorely lacking in Australia (Jolly, 2011) and must be addressed if Australia's eHealth system is to be a comparable success.

7.2.2 Current State

Australia's health care system is comprised of a complex mix of public and private care providers, funded through a combination of payments by the Australian, State and Territory Governments, private health insurance and consumers (Deloitte, 2008). Healthcare is one of Australia's largest and most complex industry sectors. In 2006, around 750,000 people were employed in the health services industry, including 39,000 general practitioners, 16,300 pharmacists and 12,700 dentists (Deloitte, 2008). As Australia's healthcare sector has grown, states and territories have been burdened with ever increasing healthcare costs. In the 1990's, the Australian Government looked at ways in which skyrocketing health expenditure could be reduced without lowering the quality of medical services; eHealth was identified as a viable solution and the concept was established.

The Australian Government has since implemented numerous pilot trials and implementation strategies that have been aimed at furthering the eHealth cause, using ICT enabled technologies to deliver safe, reliable and efficient healthcare for all Australians (EHealth, 2012). The National EHealth Transition Authority (NEHTA) was established in 2005 to coordinate these efforts on a national level (Deloitte, 2008). NEHTA has received a total of $366.2 million in federal government funding allocations to develop eHealth standards, clinical terminologies and patient and provider identifiers. This funding has been used to implement the Unique Health Identifier (UHI) service, National Authentication Service for Health (NASH), and the Personally Controlled Electronic Health Record (PCEHR) system.

Australia's eHealth strategy is currently being deployed in all states and territories, with each state and territory at different stages in the transition process. NEHTA is overseeing this transition and despite increased levels of eHealth activity at the national, state and territory levels, ranging from infrastructural initiatives to clinical information system initiatives, Australia has not been able to keep pace with developments overseas (Deloitte, 2008). Interoperability issues have caused significant delays as variations in legislation, medical systems, infrastructure, and social norms have had to be resolved at the local level in each jurisdiction. NEHTA

has successfully launched the PCEHR system, one of the more important components of eHealth, with consumers able to apply for their own record from July 1, 2012. Adoption of the PCEHR system has however been slow from consumers and healthcare providers alike - it is yet to be seen whether or not participation figures can be increased to a level that delivers the benefits initially promised.

It could be argued that although eHealth has been on the political agenda for close to two decades, the barriers initially identified are still in place today. For instance, in 1997 the Standing Committee on Family and Community Affairs concluded that the protection of patient privacy would not be affected by the introduction of electronic health records; consumer and privacy groups disagreed at the time (Jolly, 2011). In the PCEHR Concept of Operations consultation process, submissions relating to security and privacy made up almost a quarter of all those received (Jolly, 2011). Similarly, Newspoll research indicates that 41% of consumers are not confident that their personal details will remain confidential under the PCEHR system (Cresswell, 2012). Despite the Government's assurances that privacy protections and appropriate security measures are critical aspects of the PCEHR system and that a combination of technical, policy, governance and legislative safeguards will be in place to facilitate legitimate information access, these privacy concerns have yet to be resolved to consumers' full satisfaction (Jolly, 2011).

Australia's eHealth system has come a long way since its conception in the 1990's, but it remains a work in progress. Some of the more important aspects of eHealth such as the UHI service, NASH and PCEHR system have been implemented, but lack the full range of functionality initially promised. They also appear to have been developed without stakeholder engagement; as such, support for eHealth is lacking and participation rates remain dismal. Facets of eHealth are reaching a degree of maturity within their development, but without positive direction these ventures will not produce the improvements in healthcare that could be possible (Curtis, 2007).

7.2.3 Privacy vs. Information Access

In previous chapters a discussion on information privacy and information requirements in the eHealth domain was presented. Here we will restate some of the issues discussed that are relevant to the IAF.

Information Privacy

Privacy is a fundamental principle underpinning quality healthcare in Australia (Office of the Australian Privacy Commissioner, 2005). Privacy is one aspect of confidentiality (Holloway, 2004) that provides that information collected, used and stored should only be used for the purpose for which it was collected; it differs to confidentiality in that it is assumed that the subject of that information has provided it voluntarily (Whitman & Mattord, 2010). Privacy is about giving users control over how their information is managed. In the medical setting, this refers to the obligation by healthcare providers not to disclose personal information given by the patient or resulting from examination of the patient, to any other person or organisation without first obtaining consent (Holloway, 2004).

Privacy in health information systems is particularly important given the sensitivity of health information and its deeply personal nature (Office of the Australian Privacy Commissioner, 2005). Electronic health records contain sensitive personal information about a patient's sexual and mental health, addictions, abortions and an array of other diseases and illnesses that may cause embarrassment, discomfort, social isolation and effect self esteem if unlawfully disclosed. Depending on the circumstances, disclosure of this information may also affect a patient's employability or be used against them in family law matters or insurance claims (Cannoy & Salam, 2010; Pratt, et al., 2006a).

During the PCEHR system's public consultation and feedback process, privacy was one of the top two concerns raised by Australian consumers (Australian Government Department of Health and Ageing, 2011). It was found that without proper mechanisms in place to ensure that personal information remains confidential, consumers are reluctant to involve themselves in electronic health systems and may avoid treatment altogether, putting their lives or the lives of others at risk. Effective privacy measures are a key part of any successful electronic information system but are particularly important in health information systems that manage sensitive personal information. For eHealth to encourage widespread consumer participation (Jolly, 2011), more effective privacy measures must be put in place for the collection, storage or use of patient information.

Information Access

Information access in the health setting is of utmost importance, as it enables healthcare providers to make fully informed medical decisions required to correctly diagnose, treat and manage patients (Gajanayake, Iannella, & Sahama, 2012). Given the time-critical nature of healthcare, it is crucial that health information systems provide access to this information in a timely manner.

Information access falls under Pfleeger's (2003) third pillar of security, availability, which is concerned with ensuring that information is available to authorised users when they need it. Electronic information systems are often considered a double edged sword in this regard; whilst technologically capable of providing access to disparate pieces of information in a time-efficient manner, they can also be the source of unnecessary delays when the underlying security policies do not accurately reflect the goals and requirements of system users. Security policies must balance the needs of all users whilst taking into consideration the context in which the system operates if an appropriate level of information access is to be achieved.

Information access in the health setting refers to a healthcare providers ability to access all parts of a patient's complete, accurate and up-to-date health record, necessary for the given treatment scenario. Timely-access to this information in the medical environment is crucial due to the time-critical nature of healthcare and the grave consequences that delays can have on patient safety (P. A. Williams, 2007). This is particularly true of treatment scenarios where the patient is unable to provide information themselves due to injury, illness or lack of consciousness (Lehnbom, McLachlan, & Jo-anne, 2012). Without timely-access to complete patient records, healthcare providers are faced with a challenge not dissimilar to completing a jigsaw puzzle with half the pieces missing; it becomes an impossible task unless the quality is reduced.

Electronic information systems used in the health environment must ensure that information security measures assist rather than hinder healthcare providers in accessing complete patient records in a time-efficient manner. If appropriate security measures are not employed, the functionality and potential benefits of these systems will be severely limited and healthcare providers will be unable to provide the high-quality medical care that patients require.

7.2.4 Finding a Balance

All information accountability systems must balance the need for privacy with the need for information, taking into consideration user goals and requirements that are specific to the context in which the system must operate as discussed in chapter two. Within the health context, these user goals and requirements are as complex as the consequences for failing to find the correct balance are severe. Inadequate levels of information privacy can result in the unauthorised disclosure of patients' sensitive health information, while inadequate levels of information access can result in delays in treatment that put patient lives at risk.

Health information is perhaps the most intimate, personal, and sensitive of any information maintained about an individual (Gostin, 1995). Patients expect information gathered about them during episodes of medical care will remain confidential and only be used for the purposes for which it was originally collected. The primary concern of medical practices however is the welfare and treatment of patients, not the security of personal information (P. A. Williams, 2007). As such, healthcare providers need to be guaranteed that they will have timely-access to complete health records, necessary in making fully informed medical decisions as to the diagnosis, treatment and management of patients.

Information privacy and information access are competing concerns; an increase in one invariably results in a reduction in the other. For most information systems, the balance between these concerns is not critical. In the health setting however, there is no room for error as the functionality of these systems depends on the support and participation of consumers and healthcare providers alike. System developers must properly capture the intentions of users so that appropriate usage policies can be defined for data objects that accurately reflect user's strategic goals (Bresciani, et al., 2004). Failure to engage specialist healthcare knowledge in this development process is likely result in an inadequate balance between the need for privacy and the need for information that will severely limit the functionality and effectiveness of any resultant electronic health information systems.

7.3 PCEHR SYSTEM

7.3.1 Overview

Australia's eHealth system aims to provide safe, reliable and efficient healthcare for all Australians (EHealth, 2012); the Personally Controlled Electronic Health Record (PCEHR) system is a key component of the national eHealth strategy that provides patients with a single, electronic health record (EHR) that summarises the detailed information contained in local electronic medical records (EMR). The PCEHR system gives a degree of personal control to patients by allowing them to set access controls to determine which healthcare providers have access to which parts of their health record (Foo, 2012). Authorised healthcare providers are able to access patient records from anywhere in Australia, and over time patients will be able to contribute their own information to append the PCEHR health summaries (National E-Health Transition Authority, 2012). The Australian Government initially allocated $466.7 million to developing the PCEHR system but this figure has since blown out to $760 million (Dearne, 2012a). Despite the money invested in the PCEHR system to-date, it has failed to achieve widespread adoption.

The Australian PCEHR system is an opt-in system. From July 1, 2012, consumers have been able to apply for their own electronic health record online, by calling a toll free number, submitting an application in writing or at their nearest Medicare branch. In its first week of operation, only 803 consumers signed up to the PCEHR system (McDonald, 2012) – at this rate it will take over 540 years to register Australia's current population of 22.6 million. There are many reasons for this slow rate of adoption, but for the purposes of this discussion it is sufficient to look at the components of the PCEHR system that have failed to engender trust and confidence in stakeholders. Detailed discussions of the pre and post views on the PCEHR system are given next.

Pre-launch views on PCEHR

There was much hype prior to the release of the PCEHR in July 2012 by commentators concerned that such a central, personally controlled record of sensitive health information was an accident waiting to happen and a honey pot for malicious intent. Most of the concerns were related to patient safety that may be unduly affected by incomplete or inaccurate records, however fears also extended to privacy and cyber-attacks by information thieves. Chair of the AMA (WA) Council of

General Practice supported the PCEHR, provided they were implemented correctly and took into account feedback from health and information management professionals. However he raised concern over the PCEHR access controls, stating:

> "Where many will get uncomfortable is the 'access' restrictions set by consumers, which don't pass the safety, common sense or inclusiveness test. I fear that individuals could limit access wherever they like." (Wilson, 2011)

Negative view about the lack of feedback being taken onboard during the development process have been expressed (Dearne, 2012b):

> "All over the world, large-scale health IT projects have been plagued with major delays, cost overruns and a failure to deliver much in the way of improved clinical outcomes... It is disappointing that politicians have chosen to ignore the concerns of people with specific expertise in health IT and have not made substantial adjustments and corrections in response to that clear advice."

It should be noted that such negative press has been common in the pre-launch stage of other large electronic information systems worldwide, with many of the concerns later being found to be irrational as pointed out below.

> "There are International and Australian precedents for this initiative and the absurdities and initial paranoia have rationalised into what has become a good EHR, but none on such a scale."(Dearne, 2012b)

Current views on PCEHR

There are two main stakeholders that are likely to be affected by the launch of the PCEHR system; consumers (patients) and healthcare providers (organisations and professionals). While there was much speculation about how the PCEHR would work prior to their launch on July 1st 2012, since their launch only a small number of reviews as to their success have been published. This may be due to the fact that many of the fears were unwarranted, or because it is too close to the launch date for a sufficient analysis to have been made.

It is generally assumed that increasing patients' ability to view and share their medical histories will result in reductions in treatment and medication errors, and improved healthcare (Mandl, Simons, Crawford, & Abbett, 2007). However preliminary results of studies on overseas PCEHR systems, such is Indivo, reveal

that there is poor knowledge and understanding about the PCEHR among consumers that is likely to restrict uptake en masse (Lehnbom, et al., 2012).

Some of the perceived benefits of the PCHER identified by Lehnbom et al. (2012) in their study, include safer healthcare brought about by a more holistic approach, timely access to information, savings in time and costs, and easy access to information when attending to unconscious people or people with dementia. One doctor, identified only as 'Doctor 9' in the study, was quoted as saying:

> "Well the benefit is that the particular health professional that the patient is attending has a full picture of what the current situation is, whether it's with medications, whether it's with investigations, whether it's with diagnosis, so that a holistic approach can be made with patient management" (Lehnbom, et al., 2012)

While this may be true of the Indivo system, Australia's PCEHR system only gives Health and Event Summaries. This limits the usefulness of the health records as detailed raw data, necessary for doctors to make an educated and informed decision, is still stored in local medical records. An Assistant in Nursing at the Prince Charles Hospital, stated:

> "Even nurses rely on accurate and complete patient data – how can you get that sort of detail from a health summary?"

A number of concerns about PCEHRs were related to privacy, not being a complete health record, not wanting every healthcare provider to know everything and a perception that maintaining PCEHRs would be time consuming (Lehnbom, et al., 2012).

There are some noticeable differences in opinion between participants of the Lehnbom et al (2012) study with regards the benefits and concerns of PCEHRs. For instance some regarded the holistic approach as a benefit, while others considered not having a complete health record a concern. Similarly, some participants believed PCEHRs would provide timely access to information and thus save time, while others believed maintaining those records would be time consuming. This reiterates the point that there is a general lack of understanding and knowledge about PCEHRs among healthcare providers and consumers.

In another study by Weitzman et al (2009), similar results were obtained with participants demonstrating low levels of awareness about Personally Controlled Health Records (PCHR). Participants also appeared to overestimate the extent to which personal health information is available and flowing electronically within provider systems, with many assuming that such information flow already occurs.

With regards the privacy of PCHRs, it was found that a moderate level of concern about privacy existed with many participants feeling that some privacy issues were unavoidable. Several specific threats to privacy were identified including:

- Intentional identity theft;
- Disclosure and misuse of information by insurance companies;
- Accidental mix-up of records and their contents;
- Mismatch of medical records data with personal health records;
- Misuse and inappropriate viewing, including attempts by healthcare professionals to "snoop" on former patients or co-workers. (Weitzman, et al., 2009)

These perceived risks were offset by an understanding that privacy is also risked in paper information, and risks were discounted by the high value placed on ready access to health information.

Consumers expressed a high amount of interest in the concept of greater access and control of their health information, however many viewed such autonomy as a double-edged sword. Discomfort among some users about patient annotation was echoed by healthcare providers and service administrators who viewed such control as a concern in terms of quality of care, completeness of records, and risks for liability (Weitzman, et al., 2009) given the potentially serious impact of errors in the healthcare setting (P. A. Williams, 2007). It was noted that if the PCEHR was to become the sole health record, these problems may be resolved.

Healthcare providers were uncertain about responsibility for clarifying the meaning and contents of records and concerned about time requirements to address patient questions. While observed levels of problems were lower than anticipated, they were exacerbated by gaps in health and technological literacy. Providers were

not always well positioned or resourced to respond to consumers' questions and older persons in particular encountered technical barriers around system access. The large divide between lay and technical vocabularies also caused anxiety and dismay among users who saw unfamiliar or frightening content in records (Weitzman, et al., 2009).

Technological literacy also appears to be an issue with the maintenance of electronic health records by some healthcare providers. Karen Lohrey, a Head Nurse at Prince Charles Hospital stated:

> "eHealth is supposed to be good, but where I work it hasn't really filtered down to the floor staff. Many of the nurses are aged and lack computer literacy too, so they can't interact with what's there anyway. It's left to staff higher up to keep the electronic records up-to-date." (Weitzman, et al., 2009)

It is evident from these studies that a lack of understanding and knowledge about PCEHRs, together with privacy risks and the potential for incomplete or inaccurate records to adversely affect the health of consumers, is likely to limit the adoption of PCEHRs in Australia if the current system is not improved.

7.3.2 Components

Preventative Approach

Australia's PCEHR system utilises a preventative approach to information security that aims to ensure the privacy of patient's sensitive health information by imposing rigid access controls that prevent users from accessing information that they are not authorised to access. Although access controls provide an adequate level of information privacy in the business setting, it is accepted that these preventative measures are inadequate in the health setting (Feigenbaum, et al., 2012; Kagal & Abelson, 2010).

Preventative approaches that make use of rigid access controls work well in the business setting where the scenarios that may give rise to privacy breaches are predictable. Preventative measures are not suitable in the health setting however as the complexities of the health environment are dynamic and un-predictable; restricting healthcare providers from accessing complete patient records denies them the ability to make fully informed medical decisions that in turn results in reduced medical outcomes for patients (Jolly, 2011).

These preventative measures have failed to engender trust and confidence in stakeholders to date. Consumers feel burdened with the task of setting their own access controls and checking their own audit logs in order to ensure the confidentiality of their sensitive health information (Australian Healthcare and Hospitals Association, 2012). Healthcare providers are concerned that the degree of personal control given to patients will result in inaccurate and incomplete health records (Gostin, 1995). It seems unlikely that an increase in stakeholder support will occur while these preventative measures remain in force.

Rigid Access Controls

Rigid access controls are the main technological measure used to enforce the PCEHR system's preventative approach to information security. NEHTA has identified several types of roles with different capabilities in the PCEHR system; individuals, nominated representatives, authorised representatives, providers and nominated providers (National E-Health Transition Authority, 2012). These roles are used to define access controls that aim to prevent unauthorised access to patient information by healthcare providers. While successful in the business setting, the use of these access controls in the health setting has caused concern for consumers and healthcare providers alike, and contributed to the slow adoption rate of the PCEHR system.

Access controls give patients control over which healthcare providers can access which parts of their health record. There has been much concern expressed by the medical profession over the level of control given to patients in editing what information is included and what information is left out of their health summaries (Gostin, 1995), as a patient's health record must be complete and readily accessible for it to be useful to healthcare providers. Consumers should be encouraged to openly share their health information with healthcare providers. Unfortunately, privacy concerns and a lack of consumer trust remain distinct obstacles in the uptake of this approach.

While it is true that a 'break the glass' mechanism is in place in the current PCHER system that allows healthcare providers to override access controls in emergency situations, it is feared that this mechanism will only be used as a last resort. As such, situations that would benefit from access to complete patient health

records, but do not require it, are likely to result in reduced quality medical outcomes for patients.

Concern has also been expressed by consumers who fear that the access controls they implement will not adequately protect their sensitive health information (Australian Healthcare and Hospitals Association, 2012). Setting pre-emptive restrictions on what information can and cannot be accessed by healthcare providers requires specialist medical knowledge that most consumers do not possess. When consumers feel burdened with protecting their sensitive health information, or do not trust the technological measures utilised, they have a tendency to set strict access controls. This in turn denies healthcare providers timely-access to complete health records, vital when dealing with life-threatening medical situations.

Another problem with relying on rigid access controls is that information transactions may be authorised semantically, but not logically. For instance a general practitioner (GP) may be authorised to access a patient's sexual health history, but if the GP accesses this information in a period when the patient did not consult a doctor or need medical treatment, then it is likely to be an inappropriate use of information. Relying on purely preventative access controls and thus not implementing adequate after-the-fact measures, such as interactive audit logs and notifications for breach, means that inappropriate uses of this nature are not prevented by the system and are only detected if consumers are vigilante in protecting their sensitive health information.

Inactive Audit Logs

At present, all information transactions are recorded in the PCEHR system's audit logs that can be viewed by consumers via the health record portal. These logs record basic information such as the date, time, type of interaction and the IHI of the healthcare organisation, but not the individual professional responsible which is likely to make identification of inappropriate uses difficult for consumers (Consumers Health Forum of Australia, 2011). The biggest letdown however is that these audit logs are inactive; there is not automatic checking of these logs, no notifications for breaches, and consumers are unable to interact with these logs to view further details or query a particular transaction.

As discussed earlier, a particular information transaction may be authorised semantically but not logically. Inactive audit logs require consumers to be vigilante in protecting their sensitive health information, by manually checking their audit trail on a regular basis to detect any inappropriate uses not detected by the system. This requires consumers to firstly remember and then find the time to check their audit logs, and secondly, it requires them to be able to interpret the information contained in these transactions. Furthermore, if they wish to query a particular transaction they must lodge a formal complaint with the Office of the Australian Information Commissioner (OAIC).

While it is true that repeated use of the 'break the glass' mechanism is automatically monitored by the current PCEHR system, this is just one form of inappropriate use. Consumers should not be burdened with protecting their sensitive health information. Audit logs should be automatically checked, notifications provided for potential breaches and consumers should be able to interact with those audit logs to query such breaches. Inactive audit logs of the current PCEHR system do not provide any of this functionality and thus further discourage widespread adoption of eHealth in Australia.

7.4 INFORMATION ACCOUNTABILITY FRAMEWORK

7.4.1 Overview

Australia is currently in the process of implementing eHealth, an ICT enabled approach to providing safe, reliable and efficient healthcare for all Australians (EHealth, 2012). The potential benefits of eHealth are significant (Peiris, 2012), but without participation on masse from consumers and healthcare providers alike they will not be realised. It is thus imperative that a new approach to information security is implemented that increases stakeholder trust and confidence, encourages greater participation in the system and allows the Australian Government to fully capitalise on the financial benefits that eHealth has to offer.

The Information Accountability Framework (IAF) aims to alleviate the concerns of stakeholders by rectifying the information security downfalls of the current system. The IAF is an after-the-fact approach to information security that will make all uses of a patient's health information transparent, holding healthcare providers accountable for any inappropriate uses by tracking and automatically

checking all transactions against context-aware privacy policies. Potential violators will be deterred with the threat of penalties for misuse so rigid access controls will no longer be required. Instead, demarcation lines will be used that warn healthcare providers when they are about to access information that they are not authorised to access but allow them to proceed if they feel that their actions are justifiable. When potential breaches occur, notifications will be automatically sent to consumers that direct them to the transaction in question and allow them to view further details or resolve the issue using the query/response justification mechanism.

Principles of information accountability underpin the IAF. Information accountability is a fairly new concept to computer science that focuses on the way users participate in a given system and the policies associated with the data elements they use. Accountability begins where responsibility ends, extending beyond identification and allowing actions to be tied to consequences and violations to be tied to penalties (Feigenbaum, et al., 2012). The main goal of accountability systems is to be non-restrictive; they aim to provide information to legitimate users without rigid access restrictions while at the same time imposing penalties for misuse.

The IAF's after-the-fact approach will alleviate the concerns of consumers and healthcare providers alike, by providing an adequate level of information privacy without restricting healthcare providers in delivering high-quality, time-critical medical care. Eliminating the need for rigid access controls will give healthcare providers timely-access to complete health records, while the active audit logs and notifications for breach remove the burden currently imposed on consumers in ensuring the confidentiality of their sensitive health information. Both stakeholders are also likely to seek comfort from the parallels that can be drawn between the IAF and law enforcement in the offline world (Feigenbaum, 2010). By achieving a better balance between the need for information privacy and the need for information access, the IAF is likely to achieve support from consumers and healthcare providers alike, thus increasing participation levels and encouraging widespread adoption of the eHealth system.

7.4.2 Components

After-the-Fact Approach

Health information is perhaps the most intimate, personal, and sensitive of any information maintained about an individual (Gostin, 1995). Traditional approaches to information security have aimed to prevent this sensitive information from escaping beyond appropriate boundaries, with minimal measures in place to deal with breaches when they occur (Weitzner, et al., 2008). As the nation's healthcare system grows in size, scope, and integration, the susceptibility of health information to disclosure will also increase (Gostin, 1995). As such, information security measures must be implemented that aim to both prevent breaches and deal with them when they do occur. After-the-fact approaches use the principles of transparency and accountability to do just this.

Transparency provides that all relevant users must be able to observe how information is used and by whom. In the health context, this means that all uses of a patient's information by healthcare providers are visible to the required entities and can be traced back to an individual organisation or professional. Making information transactions transparent eliminates the need for strict pre-emptive access controls, as users are given an incentive to abide by the policies put in place, knowing that all transactions will be automatically checked for policy compliance (Weitzner, et al., 2008). Accountability extends beyond identification and exposure and allows actions to be tied to consequences and violations to be tied to penalties (Feigenbaum, et al., 2012). In the health setting, this means that all information transactions are tracked, checked against context-aware privacy policies and then traced back to individual healthcare providers who can then be held accountable for any misuse (Weitzner, et al., 2008).

The IAF alleviates the concerns of consumers by tracking all information transactions, automatically checking them for conformance with context-aware privacy policies, and imposing penalties on healthcare providers for proven cases of misuse; these measures ensure patient privacy. The IAF also alleviates the concerns of healthcare providers by removing the rigidity usually associated with access controls that often prevents timely-access to complete patient records necessary for making fully-informed medical decisions; these measures ensure timely and complete access to patient information. It can therefore be seen that the two

competing stakeholder concerns that have caused so much frustration in the formation of eHealth policies to date, are appropriately balanced by the IAF's after-the-fact approach and are thus likely to gain the support of consumers and healthcare providers alike.

Demarcation Lines

The IAF will still make use of access controls, but these access controls will act more as demarcation lines than rigid barriers. A trusted authority (TA) with a broad medical knowledge base will set blanket access controls that account for a multitude of different treatment scenarios. Healthcare providers will be able to access all parts of a patient's health record as is deemed appropriate by the TA, but if they choose to use that data for any non-prescribed purposes they will be required to justify their actions at a later date. This approach will still hold healthcare providers accountable for their use of patient data, but will not get in the way of their performance of time-critical medical tasks.

The primary concern of medical practices is the welfare and treatment of patients, not the security of personal information (P. A. Williams, 2007). Timely-access to this information in the medical environment is crucial due to the time-critical nature of healthcare and the grave consequences that delays can have on patient safety (P. A. Williams, 2007). This is particularly true of treatment scenarios where the patient is unable to provide information themselves due to injury, illness or lack of consciousness (Lehnbom, et al., 2012). Consumers will still be given a degree of personal control over their health record, but only to extend consent on the access controls put in place by the TA. Having a medically knowledgeable TA set the access controls will prevent problems associated with consumers implementing restrictive access controls without the specialist knowledge required to know what information is required in a given treatment scenario.

To ensure that these demarcation lines are effective and supported by the medical profession, the notifications accompanying unauthorised access will be fine-grained and give healthcare providers all the information they need to make an informed decision as to whether or not they should proceed. These notifications will also be accompanied by a non-reputable confirmation that will prevent accidental breaches and help provide data provenance for any subsequent legal actions.

Active Audit Logs

Australia's current eHealth system relies on preventative measures to ensure information privacy. As such, there are very few mechanisms in place for holding healthcare providers accountable for any inappropriate uses of a patient's sensitive health information after-the-fact. The IAF has a number of measures that provide after-the-fact functionality, one of these being active audit logs. Inactive audit logs can be used to determine *who* accessed *what* information *when* and w*here*; active audit logs utilised by the IAF will be able to provide the missing *why*.

Under the current PCEHR system, consumers are burdened with the responsibility of checking their audit logs on a regular basis (Australian Healthcare and Hospitals Association, 2012) to identify any potentially inappropriate transactions that were authorised by their access controls, but were not required for their treatment. If they wish to query the validity of a particular transaction they must lodge a formal complaint with the Office of the Australian Information Commissioner (OAIC) outside of the system. As such, these inactive audit logs do not allow for user interaction which deprives consumers of a sense of control over how their sensitive health information is being managed.

Conversely, the active audit logs used by the IAF will automatically check all transactions against context-aware privacy policies, thereby identifying potentially inappropriate uses automatically. Consumers will then be given the opportunity to view further details or query the transaction in question, and healthcare providers will be given the opportunity to resolve the issue promptly by responding with their justification. This query/response mechanism will give consumers an important sense of control over how their sensitive health information is being managed that is likely to increase their trust and confidence in the eHealth system (D.J. Solove, 2008).

In addition to providing a time-efficient and effective query/response justification mechanism, active audit logs used in the IAF will provide data provenance. Provenance is an important aspect of information accountability systems that refers to the history of transactions performed on a particular data object. Provenance allows users to decide whether or not they trust a particular set of electronic data and is crucial when holding violators accountable at a later date, as it dictates the trustworthiness of data pertaining to a particular transaction. The IAF's active audit logs will ensure data provenance, further assuring consumers that

healthcare providers will be held accountable for any inappropriate uses of their health information at a later date.

Fine-Grained Notifications

It is a requirement of any effective information system that users should be well informed. In health information systems, consumers should be notified of any potentially inappropriate uses of their sensitive health information, while healthcare providers should be informed when they are about to access data that they are not authorised to access along with the penalties for proceeding. Both stakeholders should be provided with these details by the system; fine-grained notifications fulfil this requirement under the IAF.

Under the IAF, fine-grained notifications will be automatically sent to consumers to inform them of any potentially inappropriate uses of their health information. These notifications will include a detailed description of the transaction in question that lists the date, time, healthcare professional, data element accessed and the treatment scenario that the access is likely to relate to. Providing consumers with this detailed information will allow them to make an informed decision as to whether or not the transaction in question requires justification.

Similarly, healthcare providers will be presented with notifications when they are about to access data that they are not authorised to access, that informs them of the data element they are trying to access and the penalty for proceeding. Fine-grained notifications of this nature will serve two purposes. It will ensure that healthcare providers are informed of the latest policies before an action occurs so that they are fully aware of the ramifications for not complying with these policies and it will help in facilitating non-repudiation, a significant aspect of information security.

Query/Response Justification

A key component of the IAF's active audit logs is the query/response justification mechanism. Consumers will receive automatic fine-grained notifications whenever an inappropriate use is detected by the system that will direct them to the transaction in question and allow them to view further details or query the transaction. If the consumer chooses to query the transaction, the healthcare provider in question will be required to submit a response that justifies their use of that information.

The query/response justification mechanism is premised on the notion that many of the potentially inappropriate uses will in fact be justifiable by the healthcare provider in question. Given the dynamic and complex range of treatment scenarios that occur in the health setting (Weitzner, et al., 2008), access controls cannot be set to account for all possible scenarios. Therefore, when a transaction occurs that infringes on these access controls it is not necessarily conclusive as to the validity of the transaction. The IAF's query/response justification mechanism will provide a means by which consumers and healthcare providers can resolve any potentially inappropriate uses in an informal way, without resorting to the time consuming and daunting process of lodging a formal complaint with the OAIC. Avoiding the involvement of the OAIC will also prevent healthcare providers from unfair prosecution.

The IAF's query/response mechanism will hold healthcare providers personally accountable for any inappropriate uses of a patient's health information and will give patients a sense of control by allowing them to take part in this process. Consumers will benefit from the knowledge that healthcare providers will be held personally accountable for any inappropriate uses of their sensitive health information. Healthcare providers will benefit from the ease with which potential breaches can be resolved. As such, this query/response justification mechanism is likely to be supported by consumers and healthcare providers alike.

7.5 JUSTIFYING THE IAF

eHealth is a worthwhile initiative that holds great potential for Australian healthcare. It is capable of resolving issues associated with the tyranny of distance between consumers and healthcare providers, reducing costs associated with caring for an ageing population (Peiris, 2012), and reducing errors in the treatment of patients (Jolly, 2011). eHealth initiatives have been implemented worldwide with varying degrees of success; Australia is at a critical point in its transition. Consumers are concerned about the privacy of their personal information while healthcare providers are concerned about the quality of information and their ability to access complete patient records in a timely manner. Without widespread support from both consumers and healthcare providers, the benefits of Australia's eHealth system will not be realised and the project as a whole is likely to fail (Jolly, 2011). There is however a solution that alleviates the frustrations of consumers and

healthcare providers alike while providing transparency and accountability, key components of the National eHealth strategy (Deloitte, 2008); the IAF.

Australia's eHealth system to date has been an expensive exercise; the PCEHR system alone has cost taxpayers more than $760m, far higher than the initially allocated budget of $466.7m (Dearne, 2012a). Despite the financial support, participation rates have remained dismal with only 860 consumers signing up to the PCEHR system in its first week of operation (McDonald, 2012). Healthcare providers have also been reluctant to adopt the system. If successfully implemented, eHealth could save the Australian Government not only $7.6 billion in healthcare costs, but also 5000 deaths, two million primary care and outpatient visits, 500,000 emergency department visits and 310,000 hospital visits each year by 2020 (Peiris, 2012). These benefits however are entirely dependent on participation on masse by Australian consumers and healthcare providers.

eHealth to date has failed to achieve the participation rates necessary for widespread adoption. There are many issues with the current eHealth system, some more complex than others, but many of those issues relate to the competing interests of participants in the PCEHR system. Consumers are concerned about the privacy of their personal information while healthcare providers are concerned about the quality of information and their ability to access complete patient records in a timely manner. The preventative approach to information security employed by the current PCEHR system is inadequate in the health setting (Feigenbaum, et al., 2012; Kagal & Abelson, 2010) as it places these concerns in direct competition with one another. Rigid access controls effectively form a seesaw of access rights; an increase in information privacy invariably results in a decrease in information access, and vice versa. As long as a preventative approach is employed, stakeholder concerns will continue to compete with one another and widespread support for eHealth will not be achieved.

The IAF's *after-the-fact* approach to information security is capable of providing access to information in a time-efficient manner while still maintaining an adequate level of privacy. This is achieved by making all information transactions transparent, preventing breaches with the threat of penalties (Weitzner, et al., 2008) and holding healthcare providers accountable for their actions. This approach eliminates the need for rigid access controls that can restrict healthcare providers'

from accessing complete patient records in a timely-manner, and is thus likely to alleviate healthcare provider concerns relating to information access. The IAF is also likely to alleviate consumer concerns relating to information privacy as strong parallels can be drawn between after-the-fact measures and law enforcement in the offline world (Feigenbaum, 2010).

Healthcare systems require both human and technical interaction and cannot be considered independently. Thus, increasing participation in the eHealth system will require a holistic approach that not only implements technological measures, but also educates consumers about the policies that protect their health information, and educates healthcare providers about the ways in which eHealth can assist them in accessing up-to-date, accurate and complete patient records in a timely manner. The IAF is a complete package; it provides a framework that includes technological measures such as comprehensive transaction monitoring and the query/response justification mechanism, but it also provides measures that aim to increase stakeholder trust and confidences such as active audit logs, demarcation lines and fine-grained notifications. These measures have been designed around the notions of transparency and accountability that were identified as key components of the change and adoption streams of the national eHealth strategy (Deloitte, 2008).

Without significant reform, Australia's eHealth system is unlikely to achieve widespread adoption and subsequently the benefits that were initially promised will not be realised. The IAF provides a get out of jail free card for the Australian Government, by rectifying the downfalls of the current system and adding functionality that will ensure long-term support from consumers and healthcare providers alike. It is imperative that the Australian Government seriously considers the IAF as a viable solution before the eHealth reputation becomes tarnished, and the project as a whole fails.

7.6 IMPLEMENTING THE IAF

In this section, we will present facts that support the successful implementation of the IAF within the existing infrastructure including legal requirements.

7.6.1 Legal issues relating to health information management

The developing eHealth landscape raises a number of important legal challenges, particularly in relation to the establishment of an effective system for

sharing eHealth records. The two principal areas of legal relevance are, firstly, the law of information privacy - especially within the realm of sensitive information such as health information and secondly, the appropriate governance and regulatory mechanisms necessary to manage, monitor and control the system established to provide for shared eHealth information.

Health information has existed for many years prior to the invention of computers – unauthorised disclosure of health information is not a new concept, but the introduction of electronic health information systems has made more patient data available to more healthcare providers in more geographic locations. A serious concern for information accountability systems is a lack of formal legal foundations relating to health information management in Australia. Whilst Acts like the *Privacy Act 1988* (Cth) do cover health service providers (OAIC, 2012a), they do not have national jurisdiction which is needed for the national eHealth system. Without adequate legislative measures relating to mandatory notifications and penalties for inappropriate uses of a patient's health information, the IAF will not succeed.

Confidentiality of medical information is an absolutely essential part of national healthcare reform (Gostin, 1995). Consumers that are confident that their sensitive health information will remain confidential are more likely to access the health services they need (OAIC, 2012a) without fear that their personal information will be used inappropriately. As discussed earlier, confidentiality is closely linked to privacy. Privacy is an issue that has been present in our society for many years, however it is only since the late 1990s and the widespread use of the internet that it has become a serious issue. Since this time, rapid advances in technology and electronic information sharing have outpaced advances in privacy legislation. It is not surprising therefore that current legislation does not adequately cater for information privacy.

In Australia, different states and territories have implemented different privacy legislation but there is no uniform federal law that applies to all organisations in all states and territories. The *Privacy Act 1988* (Cth) comes close to achieving national coverage, but does not bind all public health services and lacks sufficient penalties to deter potential violators. The ability of any health care system to function effectively depends in part on the accuracy, currency, completeness, and availability of health data (Gostin, 1995). In addition to privacy legislation, the Australian Government

needs to enact health information management legislation that addresses the need for mandatory data notifications and penalties for inappropriate uses of health information. Until such legislation is implemented, the development of the IAF will be hindered.

Australian information privacy law

As indicated earlier, measures relating to the protection of information privacy at the federal level are set forth in the *Privacy Act 1988* (Cth) ("Privacy Act," 1988), which establishes a comprehensive statutory scheme based on 11 Information Privacy Principles (IPPs) and 10 National Privacy Principles (NPPs) which govern the retrieval, compilation, storage and use of personal information by federal government agencies and private sector organisations respectively. Under the Act, 'health information' forms part of a subset of personal information defined as 'sensitive information' - which is given a higher level of protection under the NPPs (but not the IPPs). IPP/NPP 4 contains the fundamental "Information/data security" obligation which requires agencies and organisations to take reasonable steps to secure personal information. Monitoring and compliance functions under the Act are undertaken by the Office of the Australian Information Commissioner (OAIC).

Measures of protection provided under the *Privacy Act 1988* (Cth) are essentially limited to federal government agencies and private sector organisations. At the same time, various forms of statutory and non statutory measures exist at the State and Territory level for the protection of information privacy. This has resulted in a somewhat complex web of overlapping and inconsistent provisions inimical to the development of a comprehensive and uniform national regime of protection and control.

A nationally consistent approach to information privacy and health information management in particular is therefore vital and to that extent, the Commonwealth government's acceptance of recommendations contained in a report by the Australian Law Reform Commission (ALRC) *For Your Information: Australian Privacy Law and Practice* (Australian Law Reform Commission, 2008) promises to achieve this. Major amendments to the *Privacy Act 1988* (Cth) are now imminent, aimed at achieving national consistency in information privacy protection. The principal change will bring the IPPs and NPPS together to create one uniform set of Australian Privacy Principles (APPs), ensuring in the process that additional protections exist

for health information (as a category of sensitive information) regardless of whether it is held by government agencies or private sector organisations.

Health information is defined in the Act to include any information collected about a patient's health, including notes of symptoms, diagnosis and treatments, specialist reports and test results, appointment and billing details, prescriptions, dental records, genetic information, healthcare identifiers and any other information about a patient's race, sexuality or religion that is collected by healthcare providers (Privacy Amendment (Private Sector) Act 2000, s16(6)(1)).

Initially, the *Privacy Act 1988* (Cth) only applied to federal and ACT public organisations. However an amendment to the Act, the *Privacy Amendment (Private Sector) Act 2000* (Cth), extended the coverage of the Privacy Act to cover all private health organisations throughout Australia (OAIC, 2012a). This amendment recognises the particularly sensitive nature of health information and places extra protections around its handling, including enforcement mechanisms to deal with breaches of the privacy standards. Government organisations must comply with the 11 IPPs while private health organisations are expected to comply with the 10 NPPs. It is hoped that the *Privacy Amendment (Private Sector) Act 2000* (Cth) will complement the existing culture of confidentiality that is fundamental to many health service providers' professional practice obligations (OAIC, 2012a).

Penalties for breach of privacy legislation must be significant if they are to deter potential violators. The *Privacy Act 1988* (Cth) does not impose penalties for breach of the IPP's or NPP's. Disclosure of information is covered in section 80Q (1) but the maximum penalty is a mere 60 penalty units or 1 year imprisonment. This is not a sufficient deterrent and does not accurately reflect the serious consequences that a breach of sensitive health information can have on an individual's life. New federal legislation needs to be introduced that targets health information specifically and imposes penalties severe enough to deter potential violators before they commit a wrongful act.

More specifically in relation to eHealth, the *Personally Controlled Electronic Health Record Act 2012* (Cth.) ("Personally Controlled Electronic Health Records Act 2012," 2012) contains provisions which link that legislation with the privacy protection measures contained in the *Privacy Act 1988* (Cth.). In this respect, the OAIC becomes the independent regulator of the privacy and personal data protection

issues arising in relation to the regime established for eHealth information sharing by the PCEHR.

Regulation of the eHealth sharing regime

As indicated earlier, the second area of legal relevance concerns the need to ensure that appropriate governance and regulatory mechanisms exist to oversee, monitor and manage the eHealth sharing regime. Following the development of a number of electronic health information systems across Australia, the National E-Health Transition Authority (NEHTA) was established in 2005 as a joint initiative by the Australian, State and Territory governments. NEHTA's charter included setting national standards for the electronic collection and exchange of health information and encompassed the design of a system for Shared Electronic Health Records (SEHRs) based on the development of Unique Healthcare Identifiers (UHIs).

ALRC Report No 108 of 2008, referred to earlier, advised that the establishment of a national SEHR scheme would required the development of sufficient oversight and regulatory controls sufficient to ensure public trust and confidence in the system. Reference was made earlier to the enhanced role to be undertaken by the OAIC in relation to privacy protection arising in relation to the PCEHR. In addition to this, the OAIC will have the role of receiving and inquiring into data breaches which arise as a result of the operation of the PCEHR which the relevant entities are obliged to report. At a broader level of regulation, the PCEHR also establishes a number of entities with specific advisory and monitoring functions, including the Jurisdictional Advisory Committee and the Independent Advisory Council. The jurisdictional advisory committee is responsible for advising the system operator of the PCEHR system on matters relating to the interests of the Commonwealth, States and Territories where as the independent advisory council has the function of advising the system operator on the operation of the PCEHR system, participation of the PCEHR system, clinical, privacy and security matters relating to the operation of the PCEHR system and similar matters set down by the regulations ("Personally Controlled Electronic Health Records Act 2012," 2012).

Mandatory Notifications

For there to be widespread stakeholder support for the IAF, mechanisms must be put in place to notify healthcare providers when they are about to breach a particular privacy policy and to notify consumers when a potentially inappropriate

use of their health information has occurred. Legislation must make the implementation of these notifications mandatory for all interactions within the eHealth system.

Healthcare providers should be warned when they are trying to access information that they are not authorised to access. These warnings should require a non-reputable confirmation such as entering login details to prevent accidental dismissals of the warning messages, or inappropriate uses by healthcare providers on another healthcare providers account. Healthcare providers should also be notified of the penalties for breaching each warning, so that they are fully aware of the ramifications if they choose to ignore the message and proceed to access the unauthorised data.

Similarly, patients should be informed of any potential breaches immediately, even if it is likely that the healthcare provider in question will be able to sufficiently justify the use of that information. Notifications for breach should include specific details about the transaction such as the date, time, healthcare professional in question, data element accessed and the treatment scenario that the access is likely to relate to.

The Australian Government released a set of guidelines on data breach notification in April 2012. Data breach is defined on page 2 of the guide:

> **"Data breach** means, for the purpose of this guide, when personal information held by an agency or organisation is lost or subjected to unauthorised access, use, modification, disclosure, or other misuse." (OAIC, 2012a).

These guidelines recommend that if a data breach creates a real risk of serious harm, then the consumer affected should be notified of the breach (OAIC, 2012a). Notification is regarded by the OAIC as an important mitigation strategy that has the potential to benefit both the organisation and the individuals affected by a data breach. However caution must be exercised when issuing notifications as providing information about low risk breaches can cause undue anxiety and de-sensitise individuals to future notifications (OAIC, 2012a).

More recently, the Australian Privacy Commissioner responded to a discussion paper released by the Federal Attorney General, titled *Australian Privacy Breach Notification*:

> "Privacy breach notification is an important issue that needs community debate, and I'm sure there will be a wide range of views expressed on whether this notification should be mandatory."
> "It is very concerning that many of these incidents may be going unreported and customers are unaware that their personal information may be compromised."
> "All organisations must embed a culture that values and respects privacy. I believe that mandatory data breach notification will go some way to achieving this." (Pilgrim, 2012)

At present, organisations are encouraged but not required to notify individuals when there has been a data breach; mandatory notifications need to be enacted in legislation for them to become effective. With the release of the OAIC's guidelines, and more recently the release of the *Australian Privacy Breach Notification* paper, Australia is displaying positive signs that mandatory data breach notification laws will soon be enacted.

Penalties for Breach

For information accountability systems to be effective there must be ramifications for any inappropriate use of a patient's health information in the form of legally enforceable penalties. These penalties must be explicit; actions that constitute a breach must be clearly defined along with the penalties for each type of breach. Users should also be notified of these penalties when they are about to access data that they are not authorised to access, with the financial, professional, social or legal consequences being severe enough to deter potential violators.

Legislative measures must be implemented so that penalties associated with inappropriate use of a patient's sensitive health information in the online world are the same as they are in the offline world. The fact that the information is electronic and thus not physically tangible should not act as a barrier against prosecution. Engaging a trusted medical body such as the Australian Medical Association (AMA) in the development of these legislative measures will ensure the formation of clearly defined and precise penalties that take into consideration the complexities of the

medical environment. It will also ensure that healthcare providers are not unfairly targeted and do not refrain from accessing patient health information necessary for delivering high-quality medical care for fear of prosecution.

Resolving Cases of Potential Misuse

The IAF aims to facilitate the resolution of potential cases of misuse using the query/response justification mechanism. However for this mechanism to be effective, it must be supported by relevant legislative measures. Healthcare providers must be required by law to respond to a patient's query about a potential misuse of their health information within a reasonable time, or face the associated consequences. To avoid unfair prosecution, healthcare providers should also be reminded of their obligation to respond prior to the due date. It should be noted that although the informal query/response mechanism will be utilised, consumers will still be able to further any unsatisfactory outcomes to the OAIC for a formal investigation.

7.6.2 Legal issues related to the IAF

In this section, more specific legal requirements for the IAF and consequently for Accountable-eHealth (AeH) system implementation are discussed in detail.

Data ownership and patient control of health information

Protecting the public's interest through legislative reform and ensuring people retain control over who has access to their personal health information is crucial (OAIC, 2008). According to Australian federal legislation, health information is generally owned by the HCP who creates and manages the data. But despite this ownership by HCPs, patients retain the right to access their health records. These laws do not cover the full extent of data ownership and the information control issues with regards to health information. However, in light of the newly enacted PCEHR Act, patients can define access control settings for all their clinical documents and nominate HCPs who can access them. This offers a certain degree of ownership to the patients similar to what is required by AeH systems.

Access and use of health information

The ALRC recommends a nationally consistent policy for handling health information (Australian Law Reform Commission, 2008). In the PCEHR Act, a definition of the use and disclosure of health information in a consumer's PCEHR is given which states that the users (including HCPs) of the PCEHR system should

adhere to the access controls set by the registered consumer (patient) at all times when collecting, using and disclosing health information except in some circumstances as stated in the Act ("Personally Controlled Electronic Health Records Act 2012," 2012). Use and disclosure of health information (mostly health identifiers) is also handled by parts of the Health Identifiers Act 2010 ("Healthcare Identifiers Act," 2010).

The most significant aspect of the IAF is that health information is made available to the relevant HCP without rigid access restrictions. They also recognise explicit purposes for which data can be accessed. Even though an underlying access policy exists, an HCP is allowed to override the existing policy given his professional role. But intentional misuse is entailed by negative consequences that act as an incentive not to misuse health information. Hence the IAF require laws which explicitly define how electronic health information should be accessed and used by HCPs.

Data breach notification

Data breach notification is crucial for the IAF, since consumer trust is gained through transparency which entails that all participants are kept well informed of how information is managed. The concept of data breach takes its focus from events such as computer hacking, theft of storage equipment, the inadvertent publication of personal information and the improper decommissioning of storage equipment. However, misuse of personal information by organisational employees can also be considered a form of data breach (Burdon, et al., 2010; Kierkegaard, 2011).

Data breach notification plays a significant role in relation to information privacy law since information subjects, with certain degree of control of their information, clearly deserve the right to be informed about breaches of their personal information – particularly those occurring within specific settings such as healthcare. In terms of data breach notification generally, the Australian Government, although aware of its significance, has not been as active as other jurisdictions such as those in the US and the EU. At this stage in Australia, there has been no enactment of a general statutory data breach notification law (Burdon, Lane, & von Nessen, 2012) although one now appears imminent (see below). In the meantime and in the absence of such a law, the OAIC re-issued voluntary notification guidelines to assist and

encourage stakeholders to maintain appropriate security measures, report breaches and generally to promote a culture of notification (OAIC, 2012a).

In ALRC Report No 108 of 2008, the ALRC recommended an amendment to the *Privacy Act 1988* (Cth), to create a statutory reporting obligation based on a two-stage notification trigger requiring, firstly a reasonable expectation that there has been an unauthorised acquisition of specified personal information (which would include both personal information and sensitive personal information - such as health information) and secondly, a real risk of serious harm as a result of such disclosure to an affected individual (Recommendation 51-1).

More recently and as part of its 2nd Stage Response to ALRC Report No 108 of 2008, the Australian Government finally released a Discussion Paper, *Australian Privacy Breach Notification* (Commonwealth of Australia Attorney-General's Department, 2012) which announced the government's intention to legislate in response to the ALRC recommendation. The Paper outlines relevant issues and options with respect to the nature and wording of a mandatory data breach notification regime and invites submissions from the public.

Although the *Privacy Act 1988* (Cth) has not yet been amended to include a *general* data breach notification obligation, the Australian government was prompt in establishing a *specific* mandatory data breach notification regime for eHealth information. This regime, set forth in the PCEHR Act, establishes a legal obligation to report data breaches in the circumstances set forth in the statute. To assist stakeholders in understanding and complying with their legal obligation to report data breaches under the PCEHR system, the OAIC has published draft guidelines, *Mandatory Data Breach Notification in the eHealth Record System* (OAIC, 2012b).

Transaction logs

Earlier in the thesis, provenance was identified as a key characteristic of the IAF. Information about how data is used by HCPs is crucial especially when validating justifications by HCPs. The transaction logs of one's own EHR must be accessible to the patients. It must be clearly stated in appropriate legislation how the logs are maintained and who, how and for what reasons they can be accessed and used. Currently, the PCEHR Act identifies the access to audit logs in the PCEHR system only as a system operator's obligation. The "PCEHR concept of operation"

document however, contains detail of the consumers' rights to access audit logs (National E-Health Transition Authority, 2011a). But we contend that in the IAF (if not for the PCEHR system) the patients should also retain the right to access transaction logs in their own EHR and must be formally established through legislation.

Resolving disputes

A consumer of an AeH system, within the IAF, is entitled to make inquiries pertaining to certain usage of their health information by a HCP which the system determines that could be potentially harmful to the consumer. The HCP in question is required to make a valid justification of his or her use of the consumers' health information. It is the invalid justifications that are followed by legal penalties. The PCEHR Act defines several scenarios where participants (including HCPs) of the PCEHR system can collect, use and disclose health information outside of the access controls set by the consumers. But these scenarios are mostly for special circumstances and do not cover general use of health information, and in turn, do not cover what is required by the IAF.

In the case of a dispute between a patient and an HCP relating to inappropriate use of health information, a defined method for resolving that dispute is required. Unlike cases of medical negligence, which are already addressed by law, resolving disputes relating to health information usage are not well defined within the legal framework. A clear definition of legal penalties for misuse of information is required for the IAF because they rely heavily on deterrence trough incentives. The penalties must be unambiguously defined and expressed such that they are well understood by all participants of the system. However, without covering all other aspects relates to intentional data breaches, the definition of these penalties is unlikely.

As mentioned earlier, the IAF defines a protocol for inquiries and justifications for potential misuse of information. This acts as the initial dispute resolution protocol. Issues can be resolved if a justification given by an HCP is deemed valid by the system and if the patients concur. But there are no IAF explicit protocols defined for situations where HCPs fail to provide a valid justification. Although the IAF protocols give some incentive (in the form of transparency) for HCPs to abide by usage policies, the yet undefined penalty measures are the real accountability measures that would deter HCPs from intentionally misusing health information at

the same time increase patient confidence in sharing their health information with HCPs.

7.6.3 Stakeholder Involvement

It is suggested that one of the key reasons for the failings of the current eHealth system is that stakeholders were not involved from an early stage (Jolly, 2011, p25), with NEHTA being criticised for its 'cycle of criticism, defensiveness and isolation' (Boston Consulting Group, 2007). As a result, several aspects of the eHealth system were developed without regard for the goals and requirements of users in the medical environment that has contributed to the poor participation rates of the eHealth system to-date. Conversely, Denmark's eHealth system appears to have benefited from the high priority placed on engaging stakeholders in determining the content of health records and setting standards for data (Jolly, 2011).

While the IAF has been designed with the best interests of consumers and healthcare providers in mind, it is important to engage both parties in the development of the finished product. Increasing trust and confidence in the eHealth system is the number one priority for the IAF. It is hoped that by engaging stakeholders in the development process, the need for alterations will be mitigated as user goals and requirements will be properly captured first-time round. It is also hoped that engaging stakeholders in the development process will increase their participation in the finished system.

7.6.4 Integration with existing Infrastructure

Implementing the IAF will not require a radical overhaul of existing services and infrastructure. Already implemented services such as the PCEHR's audit logs, access controls and notification system will instead be modified to accommodate the IAF's functionality.

The PCEHR audit logs record the date, time, IHI of the healthcare organisation in question, and the type of data accessed. These logs will be modified so that the individual healthcare provider in question is identified, along with the fine-grained data element rather than just the type of information accessed. They will also be modified so that they can automatically detect potentially inappropriate transactions using a medically knowledgeable semantic database of acceptable data types, roles and uses. The query/response justification mechanism will require the

implementation of new functionality. Access controls will remain in force but will no longer be rigid, instead acting more as demarcation lines. They will also be set by a medically knowledgeable trusted authority (TA) and consumers will only be able to extend consent, not impose further restrictions.

The PCEHR's notification system, currently limited to notifying healthcare officials of repeat use of the 'break the glass' mechanism, will be modified to support fine-grained notifications. As discussed earlier, these notifications will inform healthcare providers when they are about to access information that they are not authorised to access, and inform consumers when there has been a potentially inappropriate use of their health information.

Modifying the audit logs of the current PCHER system to allow for automatic detection of potentially inappropriate uses will be the most challenging aspect of the integration process, as it will require the formation of context-aware privacy policies. These context-aware privacy policies will need to accurately map the complex relationships and interactions of the health domain without restricting the free flow of information that is necessary for high-quality medical care.

As we have already established, it is important for information systems to give users a significant degree of control over their personal information (D.J. Solove, 2008) however users should not have to agree to complex policies with unpredictable outcomes in advance. Similarly, users should not be given choices about every single request to use their personal information as the frequency of those choices may become overwhelming (Weitzner, et al., 2008) and cause unnecessary delays for authorised users legitimately trying to access information. Conversely, a lack of constraints on the initially voluntary disclosure of sensitive personal information may reduce information privacy (Sloan & Warner, 2010) and create a strong incentive for users to avoid participation in the eHealth system (Office of the Australian Privacy Commissioner, 2005). Thus, an acceptable set of privacy rules must be developed that balance the benefits of widespread information sharing against the loss of information privacy.

> "Like the emotive word 'freedom', 'privacy' means so many different things to so many different people that it has lost any precise legal connotation that it might once have had" (McCarthy, 1987).

Agreeing on a set of generally accepted privacy rules is a difficult task when dealing with several different laws, organisational procedures and social norms. If the privacy rules implemented by an accountability system are not generally accepted rules, then the accountability system is not a representation of peoples' opinions but an attempt to impose a view about what should be private (Sloan & Warner, 2010). Conversely, there is a risk that the health community will be reluctant to adopt these accountability measures if they feel they are too strict or unfairly subject healthcare providers to misconduct and negligence litigation. Thus, privacy policies must also ensure that healthcare providers are not subjected to excessive checks.

Once a set of generally accepted privacy rules have been enacted, a medically knowledgeable semantic database can be developed that maps these privacy rules to the multitude of different context-aware treatment scenarios that occur in the health setting. This database can then be used to automatically detect potential breaches, set access controls and issue fine-grained notifications.

7.7 DISCUSSION AND CONCLUSION

Australia is currently undergoing significant health reform with the establishment of eHealth, an ICT enabled approach to providing safe, reliable and efficient healthcare for all Australians (EHealth, 2012). eHealth utilises numerous technologies regarded by the ICT industry as best-practice; however the current preventative approach to information security employed by the Personally Controlled Electronic Health Record (PCEHR) system falls short of stakeholder expectations.

eHealth to date has been big on promise but light on delivery, in large part due to a lack of participation from stakeholders. Consumers are concerned that their sensitive health information will not remain private, whilst healthcare providers are concerned that rigid access controls used in the PCEHR system will prevent them from accessing complete patient records in a timely manner (P. A. Williams, 2007). eHealth has the potential to provide Australia with many well recognised benefits (Peiris, 2012) but without participation on masse from consumers and healthcare providers alike, these benefits will not be realised.

Preventative approaches to information security, such as those utilised by the current PCEHR system, are inadequate in the health setting (Feigenbaum, et al., 2012; Kagal & Abelson, 2010). Consumers are burdened with setting access controls

that require specialist medical knowledge to be implemented properly and healthcare providers are restricted from accessing complete patient health records, necessary for administering high-quality medical care. This preventative approach puts the information privacy concerns of stakeholders in direct competition with the information access concerns of healthcare providers; unless a different approach to information security is employed, stakeholder support will remain dismal.

The Information Accountability Framework (IAF) holds healthcare providers accountable for all uses of a patient's sensitive health information. By tracking all information transactions and automatically checking those transactions against the relevant privacy policies, the IAF will deter breaches with the threat of penalties instead of trying to prevent all possible breaches with pre-emptive access controls. This approach is similar to law enforcement in the offline world (Feigenbaum, 2010) and is likely to achieve a much better balance between the need for information privacy and the need for information access.

The IAF is meant to address the privacy conundrum by balancing competing concerns of healthcare stakeholders. Although the IAF, and therefore, AeH systems have not yet been fully implemented, they have the potential to operate as an effective countermeasure for privacy threats. We have demonstrated that adequate legislative foundations are critical for the IAF. Yet at this stage, it would appear that the current Australian legal framework relating to health information management falls short of what is necessary and appropriate for the proper implementation of the IAF through AeH systems.

Specifically, in order for the IAF to function effectively in the Australian context, a *privacy breach protocol* (Cavoukian, 2006) may be formulated that addresses AeH system characteristics and capabilities supported by existing and new legislation. Although some general guidance is provided by the recently updated *Guide to Handling Personal Information Security Breaches* (OAIC, 2008) and the more specific *Mandatory Data Breach Notification in the eHealth Record System* (OAIC, 2012b), there is currently no active and detailed privacy breach protocol in Australia. However, with the imminent enactment of a general data breach notification law, the foundations for developing such a protocol sufficient to underpin the IAF are slowly being laid.

The IAF is capable of rectifying the information security downfalls of the current eHealth system that have opposed widespread adoption to-date. Minimal modifications are required to the existing eHealth infrastructure for it to be implemented and, provided the appropriate legal framework is in place, it will increase stakeholder trust and confidence, encourage greater participation in the eHealth system and allow the Australian Government to fully capitalise on the financial benefits that national electronic health reform has to offer.

Closure

Chapter 8: Conclusions and Future Work

In this chapter, we present a summary of the work presented in this thesis with a list of contributions and possible future directions.

8.1 THESIS SUMMARY

This thesis has addressed the information privacy conundrum in the eHealth domain. The concept of information accountability was proposed as a solution and was successfully demonstrated to have the capabilities to address this problem. The thesis addressed five main research questions relating to eHealth requirements, information accountability, technology acceptance of stakeholders, and general applicability in an eHealth environment. Three main aspects related to information accountability were addressed in this thesis, namely: social aspects, technical aspects and legal aspects, which create an Information Accountability Framework (IAF).

eHealth is a complex and sensitive informatics domain. The main information resources in eHealth are electronic health records (EHR), which are still in their developing stages. One of the main impediments to EHR and therefore eHealth adoption was seen as information privacy concerns. Many available solutions to this problem were preventive measures that restrict access to healthcare information to the information users. But it was put forward that for a specialised, knowledge driven domain such as healthcare these preventive measures are inappropriate. Legitimate users, i.e. healthcare professionals, given their professional roles, must have the capability to access information that is both relevant and necessary for healthcare decision making. To that end, information accountability show favourable potential as a responsive conduit.

Given the embryonic state of information accountability in computer science, ICT and in eHealth, there were no guidelines that would enable system utilising information accountability to reach their intended goals. Such systems; accountable systems, enforce *appropriate-use* of information by providing incentives for information users to abide by the usage policies via *after-the-fact* accountability measures and for information owners by providing control of information and providing adequate transparency and the capability to inquire about possible

inappropriate uses of information. As regards to these goals, a series of information accountability principles were derived and were contextualised to eHealth giving rise to Accountable-eHealth (AeH) systems. AeH systems are a new form of eHealth applications where the subjects of the information have control of how their information is being used. Importantly however, the healthcare process is not hindered by this consumer control of information, like in previous approaches, due to the presence of a governing healthcare authority in the policy formulation process.

System adoption by domain stakeholders is a factor that affects eHealth applications where low adoption has seen the downfall of many systems. A two part questionnaire survey was conducted following a successful pilot survey to measure the perceived adoption and attitudes of future healthcare professionals and consumers towards AeH systems. The first phase of the survey focused on medical and health students from three academic institutes in Queensland, Australia. The results indicated that the attitudes towards the capabilities and the characteristics of the respondents were favourable. An empirical research model capable of predicting the future adoption of AeH systems was also designed and validated.

The second phase of the survey tested the same dimensions of AeH systems as the first phase but focused on the consumers' perspective with additional information privacy related aspects. Non-healthcare related students from the Queensland University of Technology (QUT) were utilised for this phase of the survey. The results revealed that information privacy concerns affect the perceived adoption of eHealth systems and the presence of information accountability measure alleviates those concerns. Although the presence of information accountability measures in the EHR system did not positively affect the adoption of the system they were highly correlated with other aspects that affected system adoption. The respondents strongly believed that information accountability measures should be present in eHealth systems that manipulate sensitive information. An empirical research model was also designed and validated. The model is capable of predicting the perceived acceptance of AeH system by eHealth consumers.

The main technical challenges relating to the use of information accountability in eHealth were identified as policy formulation, representation and management. To that end, a novel access control model was developed that is capable of capturing the eHealth stakeholder requirements such that the healthcare and privacy oriented usage

policies can be formulated. The proposed capabilities of the model were validated using a Web based prototype. The prototype was capable of handling three types of users: consumers, healthcare professionals and a representative of a healthcare authority. All relevant functionalities were demonstrated successfully.

The access control model architecture was extended to facilitate for information accountability capabilities such as transparency, misuse detection and misuse inquiries and justifications. The architecture was modelled in the model checking tool UPPAAL to validate the designed protocols. Different scenarios were simulated and the protocols were successfully validated. The policy representation and management of the architecture was done separate to model checking using an extension of the previously developed prototype.

Digital rights management (DRM) was adopted as a solution for policy representation and management in the architecture. The rights expression language (REL) used was the Open Digital Rights Language (ODRL) Version 2, which is an XML based REL. The stakeholder requirements gathered from the access control model were transformed to ODRL policies. These policies were successfully used to manage the access and usage requests by healthcare professionals, which were also represented in ODRL.

In the IAF, access to information, although governed by the usage polices set by the stakeholders, does not prevent legitimate, traceable users from accessing required information. Adequate notification is given to the users to avoid unintentional access of irrelevant information and to facilitate non-repudiation. All information transactions are recorded in the form of transaction logs. To make the logs policy-aware, the existing core model of ODRL V2 was extended to support the representation of transactions in ODRL. This additional capability made it possible for the transactions and the related policies at the time of the access be easily accessed and reasoned by end users, providing enhanced transparency.

As a final validation of the developed IAF, a case study was conducted taking to account the Australian eHealth system. The case study showed that the IAF can be successfully integrated into the existing eHealth infrastructure in Australia. It also highlighted necessary legal requirements for the IAF to be implemented in Australia.

8.2 CONTRIBUTIONS

This thesis makes a number of practical and theoretical contributions to the existing body of knowledge of information privacy in eHealth and the application of information accountability to eHealth. Following a literature review that fulfils research objective 1,

- First, we presented a set of principles that must be followed in the development of accountability systems, which successfully fulfils research objective 2 (a).
- Second, we contextualised the IA principles in the eHealth domain and a novel model for accountable-eHealth systems was presented. This successfully fulfils research objective 2 (b).
- Third, we presented the results of a survey that measured the attitudes of future healthcare professionals towards AeH systems. Thus, we successfully fulfil research objective 4 (a).
- Fourth, we presented and validated an empirical research model capable of predicting the perceived adoption of AeH system by healthcare professionals.
- Fifth, we presented the results of a survey that measured the attitudes of consumers towards AeH systems. Thus, we successfully fulfil research objective 4 (b)
- Sixth, we presented and validated an empirical research model that is capable of predicting the perceived adoption of AeH systems by consumers.
- Seventh, we presented and validated a novel access control model capable of capturing the requirements of eHealth stakeholders of eHealth systems, through which we successfully fulfil research objective 3 (a).
- Eighth, we presented and validated a technical architecture for the IAF and for AeH systems. Hence, we successfully fulfil research objective 3 (b).
- Ninth, we presented and validated a novel approach of representing usage policies in the IAF by utilising a novel extension of the DRM technology ODRL. We successfully fulfil research objective 3 (c).

- Tenth, we presented a case study of the Australian eHealth system that investigates the applicability of the developed IAF within the existing eHealth infrastructure and the legal framework. Through this, research objective 5 is fulfilled.

Collectively, the above outcomes addressed our overall research question in section 1.5.1. We conclude that information accountability can successfully address the issues related to healthcare information requirements and healthcare information privacy requirements in the eHealth context.

8.3 LIMITATIONS AND FUTURE DIRECTIONS

The contributions of this thesis had laid the foundations for AeH systems to be successfully implemented in the near future, thus fulfilling our research objective. However, there are several limitations and possible future research directions arising from this work following the limitations identified.

As mentioned earlier, in this thesis we have addressed information privacy of eHealth consumers, which is a significant barrier to eHealth adoption, and provided a solution in terms of information accountability. We put forth foundations for implementing information accountability in eHealth and introduced Accountable-eHealth systems. Although the provided insights into AeH systems are primarily based on consumer privacy, healthcare professionals' privacy concerns are also significant aspects to consider in relation to AeH system. We acknowledge this limitation and believe that this would be an attractive future direction for research. We also identify several limitations and possible future prospects of the work presented throughout several chapters.

First, the two empirical research models were validated using a student cohort, which requires them to be further confirmed with data acquired from a more suitable population. The access control protocols presented in chapter five were validated using a prototype used as a test vehicle. Although this was sufficient to establish our goals in the exploratory study presented in this thesis, we believe that the model could be tested in an actual healthcare setting using real clinical data, which could further establish the functionality of the model and highlight any limitations. Although the UPPAAL model that was presented in chapter six as a validation of the AeH system protocols demonstrated that the intended behaviour is achieved, the

model can be extended to include implementation constraints such as time for specific activities and the importance of specific activities. For example, depending on the type of misuse detected a priority level can be given for justifications, which could prove relevant in real life scenarios.

The results of our exploratory analysis of the application of information accountability in eHealth have laid the foundations for generic AeH systems to be formalised using an appropriate representation. We believe this has opened an attractive future research direction.

Some medical related aspects were assumed to be present in the development of certain aspects of the AeH system such as the relationships of EHR data types and intended purposes. A comprehensive knowledge base in the form of a semantic ontology may be developed, which would undoubtedly require the collaborative efforts of technology professionals and healthcare domain specialists. Finally, the core legal foundations relating to AeH systems were discussed in this thesis may be put forward as formal recommendations for consideration in future amendments and introduction of legislation. A possible future direction in relation to the case study presented is an investigation into the applicability of the IAF in jurisdictions other than Australia.

Bibliography

Adler-Milstein, J., & Jha, A. K. (2012). Sharing Clinical Data Electronically A Critical Challenge for Fixing the Health Care System. *JAMA: The Journal of the American Medical Association, 307*(16), 1695-1696.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50*(2), 179-211.

Al-Fedaghi, S. S. (2007). *Beyond purpose-based privacy access control*. Paper presented at the Proceedings of the eighteenth conference on Australasian database - Volume 63.

Alhaqbani, B., & Fidge, C. (2008). *Access control requirements for processing electronic health records*. Paper presented at the Proceedings of the 2007 international conference on Business process management.

Alhaqbani, B., & Fidge, C. (2009). *A time-variant medical data trustworthiness assessment model.* Paper presented at the e-Health Networking, Applications and Services, 2009. Healthcom 2009. 11th International Conference on.

Alur, R., & Dill, D. L. (1994). A theory of timed automata. *Theoretical computer science, 126*(2), 183-235.

Ancker, J. S., Edwards, A. M., Miller, M. C., & Kaushal, R. (2012). Consumer Perceptions of Electronic Health Information Exchange. *American Journal of Preventive Medicine, 43*(1), 76-80.

Ancker, J. S., Silver, M., Miller, M. C., & Kaushal, R. (2012). Consumer experience with and attitudes toward health information technology: a nationwide survey. *Journal of the American Medical Informatics Association*.

Anderson, J. G. (2006). Social, ethical and legal barriers to E-health. *International Journal of Medical Informatics, 76*(5-6), 480-483.

Angst, C. M., & Agarwal, R. (2009). Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion. [Article]. *MIS Quarterly, 33*(2), 339-370.

Annas, G. J. (2003). HIPAA Regulations — A New Era of Medical-Record Privacy? *New England Journal of Medicine, 348*(15), 1486-1490.

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International journal of Internet and enterprise management, 6*(4), 279-314.

Australian Government Department of Health and Ageing. (2004). *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*.

Australian Government Department of Health and Ageing. (2011). *Draft Concept of Operations Relating to the introduction of a Personally Controlled Electronic Health Record (PCEHR) System Analysis of Key Themes from the Public Consultation Process*.

Australian Healthcare and Hospitals Association. (2012). Electronic health records debut. Retrieved 22 September, 2012, from http://ahha.asn.au/news/electronic-health-records-debut

Australian Law Reform Commission. (2008). *For Your Information – Australian Privacy Law and Practice* (No. 108).

Ball, M. J., & Lillis, J. (2001). E-health: transforming the physician/patient relationship. *International Journal of Medical Informatics, 61*(1), 1-10.

Barclay, D., Higgins, C., & Thompson, R. (1995). The partial least squares (PLS) approach to causal modeling: personal computer adoption and use as an illustration. *Technology studies, 2*(2), 285-309.

Barlass, T. (2012, August 12). Patients reject eHealth system. *The Sydney Morning Herald*. Retrieved from http://www.smh.com.au/it-pro/government-it/patients-reject-ehealth-system-20120811-24179.html

Bayardo, R. J., & Agrawal, R. (2005, 5-8 April 2005). *Data privacy through optimal k-anonymization.* Paper presented at the Data Engineering, 2005. ICDE 2005. Proceedings. 21st International Conference on.

Beale, T., Heard, S., & Kalra, D. (2007). openEHR Architecture: Architecture Overview. *the openEHR release, 1*(2).

Beeler, G. W. (1998). HL7 Version 3—An object-oriented methodology for collaborative standards development. *International Journal of Medical Informatics, 48*(1), 151-161.

Behrmann, G., David, A., & Larsen, K. (2004). A tutorial on uppaal. *Formal methods for the design of real-time systems*, 33-35.

Berners-Lee, T., Hendler, J., & Lassila, O. (2001). The semantic web. *Scientific american, 284*(5), 28-37.

Bertino, E. (1998). Data security. *Data & Knowledge Engineering, 25*(1-2), 199-216.

Bishop, M. (2004). *Introduction to computer security*: Addison-Wesley Professional.

Blobel, B., Nordberg, R., Davis, J. M., & Pharow, P. (2006). Modelling privilege management and access control. *International Journal of Medical Informatics, 75*(8), 597-623.

Boston Consulting Group. (2007). BCG Report on the NEHTA Review. Retrieved 18 October, 2012, from http://www.nehta.gov.au/index.php?option=com_docman&task=doc_details&gid=421&Itemid=139&catid=-1

Boyd, J. (2003). Accountability (Vol. 69, pp. 599): McMurry Inc.

Bresciani, P., Perini, A., Giorgini, P., Giunchiglia, F., & Mylopoulos, J. (2004). Tropos: An Agent-Oriented Software Development Methodology. *Autonomous Agents and Multi-Agent Systems, 8*(3), 203-236.

Burdon, M., Lane, B., & von Nessen, P. (2010). The mandatory notification of data breaches: Issues arising for Australian and EU legal developments. *Computer Law & Security Review, 26*(2), 115-129.

Burdon, M., Lane, B., & von Nessen, P. (2012). Data breach notification law in the EU and Australia – Where to now? *Computer Law & Security Review, 28*(3), 296-307.

Byun, J.-W., Bertino, E., & Li, N. (2005). *Purpose based access control of complex data for privacy protection*. Paper presented at the Proceedings of the tenth ACM symposium on Access control models and technologies.

Byun, J.-W., & Li, N. (2008). Purpose based access control for privacy protection in relational database systems. *The VLDB Journal, 17*(4), 603-619.

Byun, J. W., Bertino, E., & Li, N. (2005). *Purpose based access control of complex data for privacy protection.* Paper presented at the Proceedings of the tenth ACM symposium on Access control models and technologies.

Cannoy, S. D., & Salam, A. F. (2010). A framework for health care information assurance policy and compliance. *Commun. ACM, 53*(3), 126-131.

Cavoukian, A. (2006). *What to do when faced with a privacy breach guidelines for the health sector*. Retrieved from http://hdl.handle.net/1873/1826.

Chau, P. Y. K., & Hu, P. J. H. (2002a). Examining a model of information technology acceptance by individual professionals: An exploratory study. *Journal of Management Information Systems, 18*(4), 191-230.

Chau, P. Y. K., & Hu, P. J. H. (2002b). Investigating healthcare professionals' decisions to accept telemedicine technology: an empirical test of competing theories. *Information & management, 39*(4), 297-311.

Chen, K., Chang, Y.-C., & Wang, D.-W. (2010). Aspect-oriented design and implementation of adaptable access control for Electronic Medical Records. *International Journal of Medical Informatics, 79*(3), 181-203.

Cheney, J., Chong, S., Foster, N., Seltzer, M., & Vansummeren, S. (2009). *Provenance: a future history*. Paper presented at the Proceeding of the 24th ACM SIGPLAN conference companion on Object oriented programming systems languages and applications.

Chin, W. W. (1998). The partial least squares approach for structural equation modeling.

Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Information Systems Research, 14*(2), 189-217.

Chismar, W. G., & Wiley-Patton, S. (2003). *Does the extended technology acceptance model apply to physicians.* Paper presented at the System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on.

Commonwealth of Australia Attorney-General's Department. (2012). *Australian Privacy Breach Notification*.

Compeau, D., & Higgins, C. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, 189-211.

Compeau, D., Higgins, C., & Huff, S. (1999). Social Cognitive Theory and Individual Reactions to Computing Technology: A Longitudinal Study. *MIS Quarterly, 23*(2), 145-158.

Consumers Health Forum of Australia. (2011). Consumer Forum on the Draft Personally Controlled Electronic Health Records Legislation. Retrieved 20, 2012, 2012, from https://www.chf.org.au/pdfs/rep/rep-836-PCEHRlegislation-Nov11.pdf

Cresswell, A. (2012). E-records in doubt. *The Australian*. Retrieved from http://www.theaustralian.com.au/national-affairs/e-records-in-doubt/story-fn59niix-1226117945857

Croll, P. R. (2011). Determining the privacy policy deficiencies of health ICT applications through semi-formal modelling. *International Journal of Medical Informatics, 80*(2), e32-e38.

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organisational privacy: Lessons from the choicepoint and TJX data breaches. [Article]. *MIS Quarterly, 33*(4), 673-687.

Curtis, R. (2007). What is e-health and why is it important? *ADF Health, 8*(2).

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 319-340.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1992). Extrinsic and intrinsic motivation to use computers in the workplace1. *Journal of applied social psychology, 22*(14), 1111-1132.

Dearne, K. (2012a). Labor's Personally Controlled Electronic Health Record system blows out to $760m. *The Australian*. Retrieved from http://www.theaustralian.com.au/australian-it/labors-personally-controlled-electronic-health-record-system-blows-out-to-760m/story-e6frgakx-1226283273933

Dearne, K. (2012b). Underdone e-health system to launch. *The Australian*. Retrieved from http://www.theaustralian.com.au/australian-it/government/underdone-e-health-record-system-set-for-launch/story-fn4htb9o-1226408292577

Deloitte. (2008). National E-Health Strategy. Retrieved 22 September, 2012, from http://www.health.gov.au/internet/main/publishing.nsf/content/604CF066BE48789DCA25751D000C15C7/$File/National%20eHealth%20Strategy%20final.pdf

Deluca, J. M., & Enmark, R. (2000). E-health: The changing model of healthcare. *Frontiers of Health Services Management, 17*(1), 3.

Demuynck, L., & De Decker, B. (2005). *Privacy-preserving electronic health records.* Paper presented at the Communications and Multimedia Security.

Downey, J. P., & McMurtrey, M. (2007). Introducing task-based general computer self-efficacy: An empirical comparison of three general self-efficacy instruments. *Interacting with Computers, 19*(3), 382-396.

EHealth. (2012). What is eHealth? Retrieved 2 October, 2012, from http://www.ehealthinfo.gov.au/what-is-ehealth

Emanuel, E. J., & Emanuel, L. L. (1996). What Is Accountability in Health Care? *Annals of Internal Medicine, 124*(2), 229-239.

Eriksen, S. (2002). *Designing for accountability*. Paper presented at the Proceedings of the second Nordic conference on Human-computer interaction.

Eysenbach, G. (2001). What is e-health? *Journal of Medical Internet Research, 3*(2).

Feigenbaum, J. (2010). *Accountability as a Driver of Innovative Privacy Solutions*. Paper presented at the Privacy and Innovation Symposium.

Feigenbaum, J., Freedman, M. J., Sander, T., & Shostack, A. (2002). Privacy Engineering for Digital Rights Management Systems. *Lecture Notes in Computer Science, Security and Privacy in Digital Rights Management, 2320*, 76-105

Feigenbaum, J., Hendler, J., Jaggard, A. D., Weitzner, D. J., & Wright, R. N. (2011, 11 - 17 June 2011). *Accountability and Deterrence in Online Life.* Paper presented at the WebSci Conference 11, Koblenz, Germany.

Feigenbaum, J., Jaggard, A. D., & Wright, R. (2011). *Towards a Formal Model of Accountability*. Paper presented at the New Security Paradigms Workshop.

Feigenbaum, J., Jaggard, A. D., Wright, R. N., & Xiao, H. (2012). *Systematizing "Accountability" in Computer Science*: Yale University.

Ferraiolo, D., Kuhn, D. R., & Chandramouli, R. (2003). *Role-based access control*: Artech House.

Ferreira, A., Cruz-Correia, R., Antunes, L., & Chadwick, D. (2007). Access Control: how can it improve patients' healthcare? In L. Bos & B. Blobel (Eds.), *Medical and Care Compunetics 4*.

Ferreira, A., Cruz-Correia, R., Antunes, L., Farinha, P., Oliveira-Palhares, E., Chadwick, D. W., et al. (2006). *How to break access control in a controlled manner*. Paper presented at the Computer-Based Medical Systems, 2006. CBMS 2006. 19th IEEE International Symposium on.

Ferreira, A., Shiu, S., & Baldwin, A. (2003, 26-27 June 2003). *Towards accountability for Electronic Patient Records.* Paper presented at the

Computer-Based Medical Systems, 2003. Proceedings. 16th IEEE Symposium.

Finkelstein, J., Khare, R., & Ansell, J. (2003). *Feasibility and patients' acceptance of home automated telemanagement of oral anticoagulation therapy.* Paper presented at the AMIA Annual Symposium Proceedings.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*.

Foo, F. (2012). Canberra admits PCEHR delays. *The Australian*. Retrieved from http://www.theaustralian.com.au/australian-it/government/canberra-admits-pcehr-delays/story-fn4htb9o-1226459290184

Fraser, R. (2006). *ISO 27799: Security management in health using ISO/IEC 17799.* Paper presented at the Canadian Institute for Health Information (CIHI) Partnership Conference. June 2006.

Friedman, B., & Grudin, J. (1998). *Trust and accountability: preserving human values in interactional experience.* Paper presented at the CHI 98 conference summary on Human factors in computing systems.

Friedman, B., Thomas, J. C., Grudin, J., Nass, C., Nissenbaum, H., Schlager, M., et al. (1999). *Trust me, I'm accountable: trust and accountability online.* Paper presented at the CHI'99 extended abstracts on Human factors in computing systems.

Gajanayake, R., Iannella, R., Lane, B., & Sahama, T. (2012). *Accountable-eHealth Systems: The Next Step Forward for Privacy*. Paper presented at the 1st Australian eHealth Informatics and Security Conference (AeHIS).

Gajanayake, R., Iannella, R., & Sahama, T. (2011). Sharing with Care: An Information Accountability Perspective. *Internet Computing, IEEE, 15*(4), 31-38.

Gajanayake, R., Iannella, R., & Sahama, T. (2012). *An Information Accountability Framework for Shared E-Health Policies.* Paper presented at the WWW2012 Workshop on Data Usage Management on the Web, Lyon, France.

Goldman, J., & Hudson, Z. (2000). Virtually exposed: Privacy and e-health. *Health Affairs, 19*(6), 140.

Gollman, D. (2009). *Computer Securuty*: John Wiley & Sons.

Gostin, L. O. (1995). Health information privacy. *Cornell L. Rev., 80*, 451-1756.

Graeff, T. R., & Harmon, S. (2002). Collecting and using personal data: consumers' awareness and concerns. *Journal of Consumer Marketing, 19*(4), 302-318.

Grimson, J., Grimson, W., & Hasselbring, W. (2000). The SI challenge in health care. *Commun. ACM, 43*(6), 48-55.

Groth, P., Gil, Y., Cheney, J., & Miles, S. (2012). Requirements for Provenance on the Web. *The International Journal of Digital Curation, 7*(1), 39 - 56.

Gustafson, D. H., Hawkins, R. P., Boberg, E. W., McTavish, F., Owens, B., Wise, M., et al. (2002). CHESS: 10 years of research and development in consumer health informatics for broad populations, including the underserved. *International Journal of Medical Informatics, 65*(3), 169-177.

Haas, S., Wohlgemuth, S., Echizen, I., Sonehara, N., & Müller, G. (2011). Aspects of privacy for electronic health records. *International Journal of Medical Informatics, 80*(2), e26-e31.

Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). Multivariate analysis. *Englewood: Prentice Hall International*.

Harrison, J. P., & Lee, A. (2006). The role of e-health in the changing health care environment. *Nursing Economics, 24*(6), 283-289.

Healthcare Identifiers Act(2010).
Heinssen Jr, R. K., Glass, C. R., & Knight, L. A. (1987). Assessing computer anxiety: Development and validation of the Computer Anxiety Rating Scale. *Computers in Human Behavior, 3*(1), 49-59.
Holden, R. J., & Karsh, B. T. (2009). A theoretical model of health information technology usage behaviour with implications for patient safety. *Behaviour & Information Technology, 28*(1), 21-38.
Holloway, F. (2004). Confidentiality: threats and limits. *Psychiatry, 3*(3), 11-13.
Hsu, M. H., & Chiu, C. M. (2004). Internet self-efficacy and electronic service acceptance. *Decision Support Systems, 38*(3), 369-381.
Hu, P. J. H., Chau, P. Y. K., Sheng, O. R. L., & Tam, K. Y. (1999). Examining the technology acceptance model using physician acceptance of telemedicine technology. *Journal of Management Information Systems*, 91-112.
Iannella, R. (2002). Open Digital Rights Language (ODRL) Version: 1.1.
Iannella, R. (2012). RDF/OWL Semantic Web mapping for ODRL V2.0. Retrieved 20 October, 2012, from www.w3.org/community/odrl/wiki/SemanticWeb#Ontology_Documentation
Igbaria, M., & Iivari, J. (1995). The effects of self-efficacy on computer usage. *Omega, 23*(6), 587-605.
Igbaria, M., Zinatelli, N., Cragg, P., & Cavaye, A. L. M. (1997). Personal computing acceptance factors in small firms: a structural equation model. *MIS Quarterly*, 279-305.
Ishikawa, K. (2000). Health data use and protection policy; based on differences by cultural and social environment. *International Journal of Medical Informatics, 60*(2), 119-125.
Jagadeesan, R., Jeffrey, A., Pitcher, C., & Riely, J. (2009). Towards a Theory of Accountability and Audit Computer Security – ESORICS 2009. In M. Backes & P. Ning (Eds.), (Vol. 5789, pp. 152-167): Springer Berlin / Heidelberg.
Jayasuriya, R. (1998). Determinants of microcomputer technology use: implications for education and training of health staff. *International Journal of Medical Informatics, 50*(1), 187-194.
Jimison, H., Gorman, P., Woods, S., Nygren, P., Walker, M., Norris, S., et al. (2008). Barriers and Drivers of Health Information Technology Use for the Elderly, Chronically III, and Underserved.
Jin, J., Ahn, G. J., Covington, M. J., & Zhang, X. (2008). *Toward an access control model for sharing composite electronic health record.* Paper presented at the 4th International Conference on Collaborative Computing.
Jin, J., Ahn, G. J., Hu, H., Covington, M. J., & Zhang, X. (2009). *Patient-centric authorization framework for sharing electronic health records.* Paper presented at the Proceedings of the 14th ACM symposium on Access control models and technologies.
Jolly, R. (2011). The e health revolution - easier said than done. Retrieved 25 September, 2012, from http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1112/12rp03
Kagal, L., & Abelson, H. (2010). *Access Control is an Inadequate Framework for Privacy Protection*. Paper presented at the W3C Privacy Workshop.
Kagal, L., Finin, T., & Anupam, J. (2003, 4-6 June 2003). *A policy language for a pervasive computing environment.* Paper presented at the Policies for

Distributed Systems and Networks, 2003. Proceedings. POLICY 2003. IEEE 4th International Workshop on.

Kagal, L., Finin, T., & Joshi, A. (2003). A Policy Based Approach to Security for the Semantic Web. In D. Fensel, K. Sycara & J. Mylopoulos (Eds.), (Vol. 2870, pp. 402-418): Springer Berlin / Heidelberg.

Kagal, L., & Pato, J. (2010). Preserving Privacy Based on Semantic Policy Tools. *Security & Privacy, IEEE, 8*(4), 25-30.

Kahn, S., & Sheshadri, V. (2008). Medical Record Privacy and Security in a Digital Environment. *IT Professional, 10*(2), 46-52.

Karsh, B. (2004). Beyond usability: designing effective technology implementation systems to promote patient safety. *Quality and Safety in Health Care, 13*(5), 388-394.

Kierkegaard, P. (2011). Electronic health record: Wiring Europe's healthcare. *Computer Law & Security Review, 27*(5), 503-515.

Kierkegaard, P. (2012). Medical data breaches: Notification delayed is notification denied. *Computer Law & Security Review, 28*(2), 163-183.

Kifor, T., Varga, L. Z., Vazquez-Salceda, J., Alvarez, S., Willmott, S., Miles, S., et al. (2006). Provenance in Agent-Mediated Healthcare Systems. *Intelligent Systems, IEEE, 21*(6), 38-46.

Kind, T., & Silber, T. J. (2004). Ethical Issues in Pediatric E-Health. *Clinical Pediatrics, 43*(7), 593.

Korzaan, M. L., & Boswell, K. T. (2008). The influence of personality traits and information privacy concerns on behavioral intentions. *The Journal of Computer Information Systems, 48*(4), 15-24.

Kwankam, S. Y. (2004). What e-Health can offer. *Bulletin of the World Health Organization, 82*(10), 800-802.

Lai, T. Y., Larson, E. L., Rockoff, M. L., & Bakken, S. (2008). User Acceptance of HIV TIDES—tailored interventions for management of depressive symptoms in persons living with HIV/AIDS. *Journal of the American Medical Informatics Association, 15*(2), 217-226.

Lampson, B. (2009). Privacy and security: Usable security: how to get it. *Commun. ACM, 52*(11), 25-27.

Lasagna, L. (2001). Hippocratic Oath: Modern Version; 1964. *Washington, DC: Public Broadcasting System (Nova Online), March*.

Lassila, O., & Swick, R. (1999). *Resource Description Framework (RDF) Model and Syntax Specification*.

Lehnbom, E. C., McLachlan, A., & Jo-anne, E. B. (2012). *A qualitative study of Australians' opinions about personally controlled electronic health records.* Paper presented at the Health Informatics: Building a Healthcare Future Through Trusted Information-Selected Papers from the 20th Australian National Health Informatics Conference (Hic 2012).

Lindqvist, H. (2006). Mandatory access control. *Master's Thesis in Computing Science, Umea University, Department of Computing Science, SE-901, 87*.

Lober, W., Zierler, B., Herbaugh, A., Shinstrom, S., Stolyar, A., Kim, E., et al. (2006). *Barriers to the use of a personal health record by an elderly population.* Paper presented at the AMIA Annual Symposium Proceedings.

Lonie, C., & Lyle, D. (1993). Teleradiology in NSW. *New South Wales Public Health Bulletin, 4*(10), 109-110.

Mandl, K. D., Simons, W. W., Crawford, W. C. R., & Abbett, J. M. (2007). Indivo: a personally controlled health record for health information exchange and communication. *BMC medical informatics and decision making, 7*(1), 25.

Marakas, G. M., Mun, Y. Y., & Johnson, R. D. (1998). The multilevel and multifaceted character of computer self-efficacy: Toward clarification of the construct and an integrative framework for research. *Information Systems Research, 9*(2), 126-163.

Mashima, D., & Ahamad, M. (2012). *Enabling Robust Information Accountability in E-healthcare Systems*. Paper presented at the 3rd USENIX Workshop on Health Security and Privacy.

Mashima, D., & Ahamad, M. (2012). *Enhancing accountability of electronic health record usage via patient-centric monitoring*. Paper presented at the 2nd ACM SIGHIT International Health Informatics Symposium.

McCarthy, J. T. (1987). *The rights of publicity and privacy*: C. Boardman.

McDonald, K. (2012, 09 July 2012). 803 sign up in PCEHR's first week. *Pulse+IT*.

McGuinness, D., & van Harmelen, F. (2004). OWL Web Ontology Language Overview. from http://www.w3.org/TR/owl-features/

Meingast, M., Roosta, T., & Sastry, S. (2006, Aug. 30 2006-Sept. 3 2006). *Security and Privacy Issues with Health Care Information Technology.* Paper presented at the Engineering in Medicine and Biology Society, 2006. EMBS '06. 28th Annual International Conference of the IEEE.

Mercuri, R. T. (2004). The HIPAA-potamus in health care data security. *Communications of the ACM, 47*(7), 25-28.

Miller, R. H., & Sim, I. (2004). Physicians' Use Of Electronic Medical Records: Barriers And Solutions. [Article]. *Health Affairs, 23*(2), 116-126.

Mills, W. (2007). Building the bridge between caring and technology. *Healthcare Information Management & Communications Canada, 21*(2), 10 - 12, 14.

Moreau, L., Groth, P., Miles, S., Vazquez-Salceda, J., Ibbotson, J., Jiang, S., et al. (2008). The provenance of electronic data. *Commun. ACM, 51*(4), 52-58.

Motta, G. H. M. B., & Furuie, S. S. (2003). A contextual role-based access control authorization model for electronic patient record. *Information Technology in Biomedicine, IEEE Transactions on, 7*(3), 202-207.

Naikuo, Y., Howard, B., & Ning, Z. (2007). *A Purpose-Based Access Control Model*.

National E-Health Transition Authority. (2011a). Concept of Operations: Relating to the introduction of a personally controlled electronic health record (PCEHR) system. Retrieved 20 September, 2012, from http://www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/PCEHRS-Intro-toc#.T9BeK8VIuSo

National E-Health Transition Authority. (2011b). The National E-Health Transaction Authority Strategic Plan. Retrieved Febuary 16, 2011, from http://www.nehta.gov.au/about-us/strategy

National E-Health Transition Authority. (2011c). NEHTA BluePrint. Retrieved 20 September, 2012, from http://www.nehta.gov.au/connecting-australia/ehealth-architecture

National E-Health Transition Authority. (2012). What is a PCEHR? Retrieved 12 August, 2012, from http://www.nehta.gov.au/ehealth-implementation/what-is-a-pcher

Neubauer, T., & Heurix, J. (2011). A methodology for the pseudonymization of medical data. *International Journal of Medical Informatics, 80*(3), 190-204.

Ni, Q., Bertino, E., Lobo, J., Brodie, C., Karat, C.-M., Karat, J., et al. (2010). Privacy-aware role-based access control. *ACM Trans. Inf. Syst. Secur., 13*(3), 1-31.

OAIC. (2008). *Guide to handling personal information security breaches*.

OAIC. (2012a). *Data breach notification*. Retrieved from http://www.oaic.gov.au/publications/guidelines/privacy_guidance/Data_breach_notification_guide_April2012FINAL.pdf.

OAIC. (2012b). *Mandatory data breach notification in the eHealth record system*.

ODRL Initiative. (2012). ODRL V2.0 - Core Model - Working Draft. from http://www.w3.org/community/odrl/two/model/

OECD. (1980). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. 2011, from http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html

Office of Legislative Drafting and Publishing. (2010). *Healthcare Identifiers Act*.

Office of the Australian Privacy Commissioner. (2005). *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*.

Or, C. K. L., & Karsh, B. T. (2009). A systematic review of patient acceptance of consumer health information technology. *Journal of the American Medical Informatics Association, 16*(4), 550-560.

Osborn, S. (1997). *Mandatory access control and role-based access control revisited.* Paper presented at the Proceedings of the second ACM workshop on Role-based access control.

Parks, R., Chu, C.-H., & Xu, H. (2011). *Healthcare Information Privacy Research: Iusses, Gaps and What Next?* Paper presented at the Americas Conference on Information Systems. Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1177&context=amcis2011_submissions

Peiris, D. (2012). Getting E-Health Right. Retrieved 23 September, 2012, from http://www.georgeinstitute.org/news-and-events/news/getting-e-health-right

Perera, G., Holbrook, A., Thabane, L., Foster, G., & Willison, D. J. (2011). Views on health information sharing and privacy from primary care practices using electronic medical records. *International Journal of Medical Informatics, 80*(2), 94-101.

Personally Controlled Electronic Health Records Act 2012(2012).

Petkovic, M., & Ibraimi, L. (2011). Privacy and Security in e-Health Applications. In C. Röcker & M. Ziefle (Eds.), *E-Health, Assistive Technologies and Applications for Assisted Living: Challenges and Solutions* (pp. 23-48).

Pfleeger, C. P., & Pfleeger, S. L. (2003). *Security in computing*: Prentice Hall.

Pilgrim, T. (2012). *Comments on Discussion paper entitled: Australian Privacy Breach Notification*.

Pratt, W., Unruh, K., Civan, A., & Skeels, M. M. (2006a). Personal health information management. *Communications of the ACM, 49*(1), 51-55.

Pratt, W., Unruh, K., Civan, A., & Skeels, M. M. (2006b). Personal health information management. *Commun. ACM, 49*(1), 51-55.

Privacy Act(1988).

Prud'hommeaux, E., & Seaborne, A. (2008, 15 January 2008). SPARQL Query Language for RDF. 2012, from http://www.w3.org/TR/rdf-sparql-query/

Ray, P., & Wimalasiri, J. (2006, Aug. 30 2006-Sept. 3 2006). *The Need for Technical Solutions for Maintaining the Privacy of EHR.* Paper presented at the Engineering in Medicine and Biology Society, 2006. EMBS '06. 28th Annual International Conference of the IEEE.

Richardson, S., & Asthana, S. (2006). Inter-agency Information Sharing in Health and Social Care Services: The Role of Professional Culture. *British Journal of Social Work, 36*(4), 657-669.

Ringle, C. M., Wende, S., & Will, S. (2005). SmartPLS 2.0 (M3) Beta (Version 2.0). Hamburg.

Rogers, A., & Mead, N. (2004). More than technology and access: primary care patients' views on the use and non-use of health information in the Internet age. *Health & social care in the community, 12*(2), 102-110.

Rogers, E. M. (1995). *Diffusion of innovations*: Simon and Schuster.

Røstad, L. (2008). *Access Control in Healthcare Information Systems.* Norwegian University of Science and Technology, Trondheim.

Sadan, B. (2001). Patient data confidentiality and patient rights. *International Journal of Medical Informatics, 62*(1), 41-49.

Salim, F., Dulleck, U., Reid, J., & Dawson, E. (2011). *Optimal budget allocation in budget-based access control.* Paper presented at the Availability, Reliability and Security (ARES), 2011 Sixth International Conference on.

Salim, F., Reid, J., Dawson, E., & Dulleck, U. (2011). *An approach to access control under uncertainty.* Paper presented at the Availability, Reliability and Security (ARES), 2011 Sixth International Conference on.

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *Computer, 29*(2), 38-47.

Sandhu, R. S., & Samarati, P. (1994). Access control: principle and practice. *Communications Magazine, IEEE, 32*(9), 40-48.

Schaper, L. (2009). *A model of information and communication technology acceptance and utilisation by occupational therapists.* Curtin University of Technology, Perth.

Schaper, L., & Pervan, G. (2007). ICT and OTs: A model of information and communication technology acceptance and utilisation by occupational therapists. *International Journal of Medical Informatics, 76*, S212-S221.

Schepers, J., & Wetzels, M. (2007). A meta-analysis of the technology acceptance model: Investigating subjective norm and moderation effects. *Information & management, 44*(1), 90-103.

Schloeffel, P., Beale, T., Hayworth, G., Heard, S., & Leslie, H. (2006). The relationship between CEN 13606, HL7, and openEHR. *HIC 2006 and HINZ 2006: Proceedings, 24*.

Scott, J. (2010). The Impact of the E-Health (Personal Health Information Access and Protection of Privacy) Act. *Canadian Journal of Administrative Law and Practice, Volume 23*(Issue 1), 55.

Simonson, M. R., Maurer, M., Montag-Torardi, M., & Whitaker, M. (1987). Development of a standardized test of computer literacy and a computer anxiety index. *Journal of educational computing research, 3*(2), 231-247.

Slamanig, D., & Stingl, C. (2010). Electronic Health Records: An Enhanced Security Paradigm to Preserve Patient's Privacy. *Biomedical Engineering Systems and Technologies*, 369-380.

Sloan, R. H., & Warner, R. (2010). Developing Foundations for Accountability Systems: Informational Norms and Context-Sensitive Judgments. *Annual*

Computer Security Applications Conference, Workshop on Governance of Technology, Information, and Policies, 2010.

Smith, H. J. (1993). Privacy policies and practices: inside the organizational maze. *Communications of the ACM, 36*(12), 104-122.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly*, 167-196.

Solove, D. J. (2008). Understanding Privacy. *Daniel J. Solove, UNDERSTANDING PRIVACY, Harvard University Press, May 2008*.

Solove, D. J. (2008). *Understanding privacy* (Vol. 10): Harvard University Press.

SPSS Inc. (2012). Statistical Package for Social Sciences (SPSS) (Version Version 19.0). Chicago, IL.

Stoop, A. P., van't Riet, A., & Berg, M. (2004). Using information technology for patient education: realizing surplus value? *Patient education and counseling, 54*(2), 187-195.

Straub, D. (1989). Validating instruments in MIS research. *MIS Quarterly*, 147-169.

Straub, D., M. C. Boudreau, M. C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems, 13*(24), 380-427.

Sun, H., & Zhang, P. (2006). The role of moderating factors in user technology acceptance. *International Journal of Human-Computer Studies, 64*(2), 53-78.

Sun, L., Wang, H., Soar, J., & Rong, C. (2012). Purpose based access control for privacy protection in e-healthcare services. *Journal of Software, 7*(11), 2443-2449.

Sweeney, L. (2002). Achieving k-anonymity privacy protection using generalization and suppression. *Int. J. Uncertain. Fuzziness Knowl.-Based Syst., 10*(5), 571-588.

Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research, 6*(2), 144-176.

The Standards and Interoperability Framework. (2012). Data Segmentation for Privacy. Retrieved 11 November, 2012, from http://wiki.siframework.org/Data+Segmentation+for+Privacy+Homepage

Thompson, R. L., Higgins, C. A., & Howell, J. M. (1991). Personal Computing: Toward a Conceptual Model of Utilization. *MIS Quarterly, 15*(1), 125-143.

Tonti, G., Bradshaw, J., Jeffers, R., Montanari, R., Suri, N., & Uszok, A. (2003). Semantic Web Languages for Policy Representation and Reasoning: A Comparison of KAoS, Rei, and Ponder. In D. Fensel, K. Sycara & J. Mylopoulos (Eds.), (Vol. 2870, pp. 419-437): Springer Berlin / Heidelberg.

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research, 22*(2), 254-268.

Tsang, E. W. K. (2002). Acquiring knowledge by foreign partners from international joint ventures in a transition economy: learning-by-doing and learning myopia. *Strategic Management Journal, 23*(9), 835-854.

Turilli, M., & Floridi, L. (2009). The ethics of information transparency. [10.1007/s10676-009-9187-9]. *Ethics and Information Technology, 11*(2), 105-112.

Vaandrager, F. (2011). A First Introduction to uppaal. *Deliverable no.: D5. 12 Title of Deliverable: Industrial Handbook*, 18.

van der Linden, H., Kalra, D., Hasman, A., & Talmon, J. (2009). Inter-organizational future proof EHR systems: A review of the security and privacy related issues. *International Journal of Medical Informatics, 78*(3), 141-160.

Venkatesh, V., & Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science, 46*(2), 186-204.

Venkatesh, V., Morris, M. G., Gordon, B. D., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly, 27*(3), 425-478.

Weber-Jahnke, J. H., & Obry, C. (2012). Protecting privacy during peer-to-peer exchange of medical documents. *Information systems frontiers, 14*(1), 87-104.

Weitzman, E. R., Kaci, L., & Mandl, K. D. (2009). Acceptability of a personally controlled health record in a community-based setting: implications for policy and design. *Journal of Medical Internet Research, 11*(2).

Weitzner, D. J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., & Sussman, G. J. (2008). Information accountability. *Commun. ACM, 51*(6), 82-87.

Weitzner, D. J., Abelson, H., Berners-lee, T., Hanson, C., Hendler, J., Kagal, L., et al. (2006). Transparent accountable data mining: New strategies for privacy protection.

Westin, A. (1967). *Privacy and Freedom*: New York Atheneum.

Whiddett, R., Hunter, I., Engelbrecht, J., & Handy, J. (2006a). Patients' attitudes towards sharing their health information. *International Journal of Medical Informatics, 75*(7), 530-541.

Whiddett, R., Hunter, I., Engelbrecht, J., & Handy, J. (2006b). Patients' attitudes towards sharing their health information. *International Journal of Medical Informatics, 75*(7), 530-541.

Whitman, M. E., & Mattord, H. J. (2010). *Management of information security*: Course Technology Ptr.

Whitten, P. S., & Richardson, J. D. (2002). A scientific approach to the assessment of telemedicine acceptance. *Journal of telemedicine and telecare, 8*(4), 246-248.

Wilkowska, W., & Ziefle, M. (2011). *Perception of privacy and security for acceptance of E-health technologies: Exploratory analysis for diverse user groups.* Paper presented at the Pervasive Computing Technologies for Healthcare (PervasiveHealth), 2011 5th International Conference on.

Williams, P. (2011). *Why Australia's e-health system will be a vulnerable national asset*. Paper presented at the 2nd International Cyber Resilience conference.

Williams, P., Nicholas, D., & Huntington, P. (2003). Non use of health information kiosks examined in an information needs context. *Health Information & Libraries Journal, 20*(2), 95-103.

Williams, P. A. (2007). *Medical insecurity: when one size does not fit all*. Paper presented at the 5th Australian Information Security Management Conference.

Wilson, S. (2011). The personally controlled health record what could it mean for us all? *Medicus, 51*(11), 13.

World Health Organisation. (2012). eHealth at WHO. Retrieved 01 August, 2012, from http://www.who.int/ehealth/about/en/

Xie, B., Dilts, D. M., & Shor, M. (2006). The physician-patient relationship: the impact of patient-obtained medical information: Health Economics.

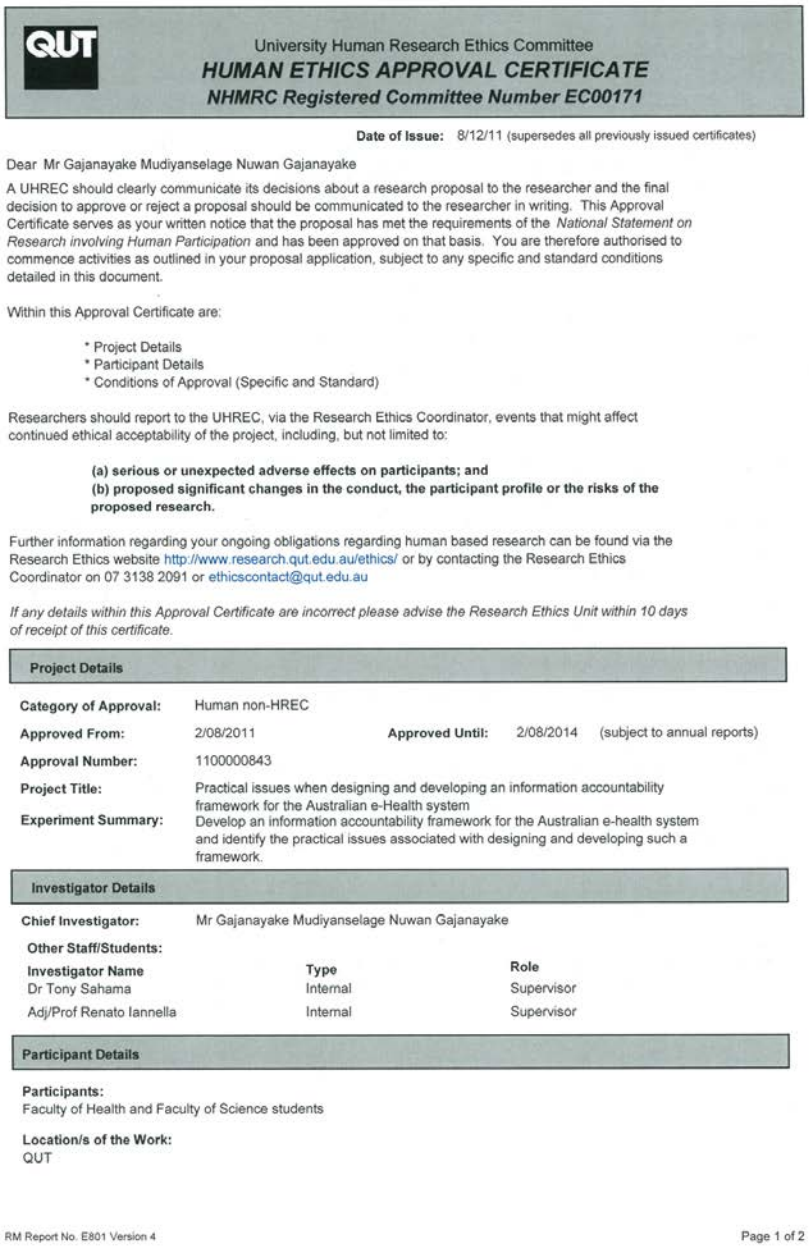
Yaffee, A. (2011). Financing the Pulp to Digital Phenomenon. *Journal of Health & Biomedical Law, Volume 7*(Issue 2), 325-372.

Yang, N., Barringer, H., & Zhang, N. (2007). *A purpose-based access control model.* Paper presented at the Information Assurance and Security, 2007. IAS 2007. Third International Symposium on.

Appendices

Appendix A
Survey - Ethical Clearance Certificates

The ethical clearance certificates for the surveys are given below.



QUT

University Human Research Ethics Committee

HUMAN ETHICS APPROVAL CERTIFICATE

NHMRC Registered Committee Number EC00171

Date of Issue: 8/12/11 (supersedes all previously issued certificates)

Dear Mr Gajanayake Mudiyanselage Nuwan Gajanayake

A UHREC should clearly communicate its decisions about a research proposal to the researcher and the final decision to approve or reject a proposal should be communicated to the researcher in writing. This Approval Certificate serves as your written notice that the proposal has met the requirements of the *National Statement on Research involving Human Participation* and has been approved on that basis. You are therefore authorised to commence activities as outlined in your proposal application, subject to any specific and standard conditions detailed in this document.

Within this Approval Certificate are:

* Project Details
* Participant Details
* Conditions of Approval (Specific and Standard)

Researchers should report to the UHREC, via the Research Ethics Coordinator, events that might affect continued ethical acceptability of the project, including, but not limited to:

(a) serious or unexpected adverse effects on participants; and
(b) proposed significant changes in the conduct, the participant profile or the risks of the proposed research.

Further information regarding your ongoing obligations regarding human based research can be found via the Research Ethics website http://www.research.qut.edu.au/ethics/ or by contacting the Research Ethics Coordinator on 07 3138 2091 or ethicscontact@qut.edu.au

If any details within this Approval Certificate are incorrect please advise the Research Ethics Unit within 10 days of receipt of this certificate.

Project Details

Category of Approval:	Human non-HREC			
Approved From:	2/08/2011	**Approved Until:**	2/08/2014	(subject to annual reports)
Approval Number:	1100000843			
Project Title:	Practical issues when designing and developing an information accountability framework for the Australian e-Health system			
Experiment Summary:	Develop an information accountability framework for the Australian e-health system and identify the practical issues associated with designing and developing such a framework.			

Investigator Details

Chief Investigator: Mr Gajanayake Mudiyanselage Nuwan Gajanayake

Other Staff/Students:

Investigator Name	Type	Role
Dr Tony Sahama	Internal	Supervisor
Adj/Prof Renato Iannella	Internal	Supervisor

Participant Details

Participants:
Faculty of Health and Faculty of Science students

Location/s of the Work:
QUT

RM Report No. E801 Version 4

Page 1 of 2

Figure A.1 Ethics certificate for pilot survey – page 1

University Human Research Ethics Committee

HUMAN ETHICS APPROVAL CERTIFICATE

NHMRC Registered Committee Number EC00171

Date of Issue: 8/12/11 (supersedes all previously issued certificates)

Conditions of Approval

Specific Conditions of Approval:
No special conditions placed on approval by the UHREC. Standard conditions apply.

Standard Conditions of Approval:
The University's standard conditions of approval require the research team to:

1. Conduct the project in accordance with University policy, NHMRC / AVCC guidelines and regulations, and the provisions of any relevant State / Territory or Commonwealth regulations or legislation;

2. Respond to the requests and instructions of the University Human Research Ethics Committee (UHREC);

3. Advise the Research Ethics Coordinator immediately if any complaints are made, or expressions of concern are raised, in relation to the project;

4. Suspend or modify the project if the risks to participants are found to be disproportionate to the benefits, and immediately advise the Research Ethics Coordinator of this action;

5. Stop any involvement of any participant if continuation of the research may be harmful to that person, and immediately advise the Research Ethics Coordinator of this action;

6. Advise the Research Ethics Coordinator of any unforeseen development or events that might affect the continued ethical acceptability of the project;

7. Report on the progress of the approved project at least annually, or at intervals determined by the Committee;

8. (Where the research is publicly or privately funded) publish the results of the project is such a way to permit scrutiny and contribute to public knowledge; and

9. Ensure that the results of the research are made available to the participants.

Modifying your Ethical Clearance:
Requests for variations must be made via submission of a Request for Variation to Existing Clearance Form (http://www.research.qut.edu.au/ethics/forms/hum/var/var.jsp) to the Research Ethics Coordinator. Minor changes will be assessed on a case by case basis.

It generally takes 7-14 days to process and notify the Chief Investigator of the outcome of a request for a variation.

Major changes, depending upon the nature of your request, may require submission of a new application.

Audits:
All active ethical clearances are subject to random audit by the UHREC, which will include the review of the signed consent forms for participants, whether any modifications / variations to the project have been approved, and the data storage arrangements.

End of Document

RM Report No. E801 Version 4

Page 2 of 2

Figure A.2 Ethics certificate for pilot survey – page 2

University Human Research Ethics Committee

HUMAN ETHICS APPROVAL CERTIFICATE

NHMRC Registered Committee Number EC00171

Date of Issue: 11/1/12 (supersedes all previously issued certificates)

Dear Mr Gajanayake Mudiyanselage Nuwan Gajanayake

A UHREC should clearly communicate its decisions about a research proposal to the researcher and the final decision to approve or reject a proposal should be communicated to the researcher in writing. This Approval Certificate serves as your written notice that the proposal has met the requirements of the *National Statement on Research involving Human Participation* and has been approved on that basis. You are therefore authorised to commence activities as outlined in your proposal application, subject to any specific and standard conditions detailed in this document.

Within this Approval Certificate are:

* Project Details
* Participant Details
* Conditions of Approval (Specific and Standard)

Researchers should report to the UHREC, via the Research Ethics Coordinator, events that might affect continued ethical acceptability of the project, including, but not limited to:

(a) serious or unexpected adverse effects on participants; and
(b) proposed significant changes in the conduct, the participant profile or the risks of the proposed research.

Further information regarding your ongoing obligations regarding human based research can be found via the Research Ethics website http://www.research.qut.edu.au/ethics/ or by contacting the Research Ethics Coordinator on 07 3138 2091 or ethicscontact@qut.edu.au

If any details within this Approval Certificate are incorrect please advise the Research Ethics Unit within 10 days of receipt of this certificate.

Project Details

Category of Approval:	Human non-HREC			
Approved From:	2/08/2011	**Approved Until:**	2/08/2014	(subject to annual reports)
Approval Number:	1100000843			
Project Title:	Practical issues when designing and developing an information accountability framework for the Australian e-Health system			
Experiment Summary:	Develop an information accountability framework for the Australian e-health system and identify the practical issues associated with designing and developing such a framework.			

Investigator Details

Chief Investigator: Mr Gajanayake Mudiyanselage Nuwan Gajanayake

Other Staff/Students:

Investigator Name	Type	Role
Dr Tony Sahama	Internal	Supervisor
Adj/Prof Renato Iannella	Internal	Supervisor

Participant Details

Participants:
Faculty of Health and Faculty of Science students

Location/s of the Work:
QUT, University of Queensland, Griffith University, Bond University and James Cook University

Figure A.3 Ethics certificate for survey phase 1 – page 1

University Human Research Ethics Committee

HUMAN ETHICS APPROVAL CERTIFICATE

NHMRC Registered Committee Number EC00171

Date of Issue: 11/1/12 (supersedes all previously issued certificates)

Conditions of Approval

Specific Conditions of Approval:
No special conditions placed on approval by the UHREC. Standard conditions apply.

Standard Conditions of Approval:
The University's standard conditions of approval require the research team to:

1. Conduct the project in accordance with University policy, NHMRC / AVCC guidelines and regulations, and the provisions of any relevant State / Territory or Commonwealth regulations or legislation;

2. Respond to the requests and instructions of the University Human Research Ethics Committee (UHREC);

3. Advise the Research Ethics Coordinator immediately if any complaints are made, or expressions of concern are raised, in relation to the project;

4. Suspend or modify the project if the risks to participants are found to be disproportionate to the benefits, and immediately advise the Research Ethics Coordinator of this action;

5. Stop any involvement of any participant if continuation of the research may be harmful to that person, and immediately advise the Research Ethics Coordinator of this action;

6. Advise the Research Ethics Coordinator of any unforeseen development or events that might affect the continued ethical acceptability of the project;

7. Report on the progress of the approved project at least annually, or at intervals determined by the Committee;

8. (Where the research is publicly or privately funded) publish the results of the project is such a way to permit scrutiny and contribute to public knowledge; and

9. Ensure that the results of the research are made available to the participants.

Modifying your Ethical Clearance:
Requests for variations must be made via submission of a Request for Variation to Existing Clearance Form (http://www.research.qut.edu.au/ethics/forms/hum/var/var.jsp) to the Research Ethics Coordinator. Minor changes will be assessed on a case by case basis.

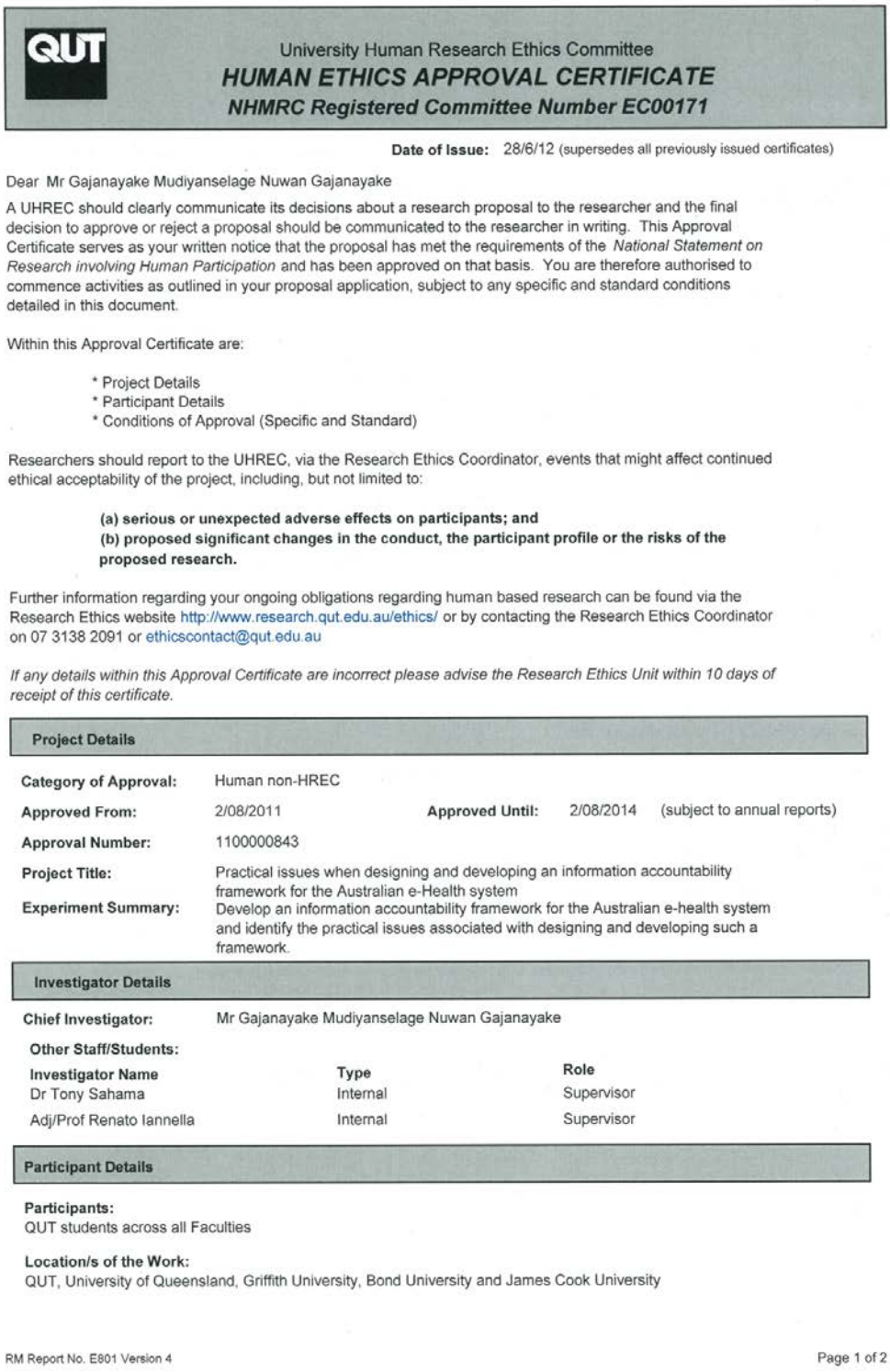
It generally takes 7-14 days to process and notify the Chief Investigator of the outcome of a request for a variation.

Major changes, depending upon the nature of your request, may require submission of a new application.

Audits:
All active ethical clearances are subject to random audit by the UHREC, which will include the review of the signed consent forms for participants, whether any modifications / variations to the project have been approved, and the data storage arrangements.

End of Document

Figure A.4 Ethics certificate for survey phase 1 – page 2



University Human Research Ethics Committee

HUMAN ETHICS APPROVAL CERTIFICATE

NHMRC Registered Committee Number EC00171

Date of Issue: 28/6/12 (supersedes all previously issued certificates)

Dear Mr Gajanayake Mudiyanselage Nuwan Gajanayake

A UHREC should clearly communicate its decisions about a research proposal to the researcher and the final decision to approve or reject a proposal should be communicated to the researcher in writing. This Approval Certificate serves as your written notice that the proposal has met the requirements of the *National Statement on Research involving Human Participation* and has been approved on that basis. You are therefore authorised to commence activities as outlined in your proposal application, subject to any specific and standard conditions detailed in this document.

Within this Approval Certificate are:

* Project Details
* Participant Details
* Conditions of Approval (Specific and Standard)

Researchers should report to the UHREC, via the Research Ethics Coordinator, events that might affect continued ethical acceptability of the project, including, but not limited to:

(a) serious or unexpected adverse effects on participants; and
(b) proposed significant changes in the conduct, the participant profile or the risks of the proposed research.

Further information regarding your ongoing obligations regarding human based research can be found via the Research Ethics website http://www.research.qut.edu.au/ethics/ or by contacting the Research Ethics Coordinator on 07 3138 2091 or ethicscontact@qut.edu.au

If any details within this Approval Certificate are incorrect please advise the Research Ethics Unit within 10 days of receipt of this certificate.

Project Details

Category of Approval:	Human non-HREC			
Approved From:	2/08/2011	**Approved Until:**	2/08/2014	(subject to annual reports)
Approval Number:	1100000843			
Project Title:	Practical issues when designing and developing an information accountability framework for the Australian e-Health system			
Experiment Summary:	Develop an information accountability framework for the Australian e-health system and identify the practical issues associated with designing and developing such a framework.			

Investigator Details

Chief Investigator: Mr Gajanayake Mudiyanselage Nuwan Gajanayake

Other Staff/Students:

Investigator Name	Type	Role
Dr Tony Sahama	Internal	Supervisor
Adj/Prof Renato Iannella	Internal	Supervisor

Participant Details

Participants:
QUT students across all Faculties

Location/s of the Work:
QUT, University of Queensland, Griffith University, Bond University and James Cook University

RM Report No. E601 Version 4

Page 1 of 2

Figure A.5 Ethics certificate for survey phase 2 – page 1

University Human Research Ethics Committee

HUMAN ETHICS APPROVAL CERTIFICATE

NHMRC Registered Committee Number EC00171

Date of Issue: 28/6/12 (supersedes all previously issued certificates)

Conditions of Approval

Specific Conditions of Approval:
No special conditions placed on approval by the UHREC. Standard conditions apply.

Standard Conditions of Approval:
The University's standard conditions of approval require the research team to:

1. Conduct the project in accordance with University policy, NHMRC / AVCC guidelines and regulations, and the provisions of any relevant State / Territory or Commonwealth regulations or legislation;

2. Respond to the requests and instructions of the University Human Research Ethics Committee (UHREC);

3. Advise the Research Ethics Coordinator immediately if any complaints are made, or expressions of concern are raised, in relation to the project;

4. Suspend or modify the project if the risks to participants are found to be disproportionate to the benefits, and immediately advise the Research Ethics Coordinator of this action;

5. Stop any involvement of any participant if continuation of the research may be harmful to that person, and immediately advise the Research Ethics Coordinator of this action;

6. Advise the Research Ethics Coordinator of any unforeseen development or events that might affect the continued ethical acceptability of the project;

7. Report on the progress of the approved project at least annually, or at intervals determined by the Committee;

8. (Where the research is publicly or privately funded) publish the results of the project is such a way to permit scrutiny and contribute to public knowledge; and

9. Ensure that the results of the research are made available to the participants.

Modifying your Ethical Clearance:
Requests for variations must be made via submission of a Request for Variation to Existing Clearance Form (http://www.research.qut.edu.au/ethics/forms/hum/var/var.jsp) to the Research Ethics Coordinator. Minor changes will be assessed on a case by case basis.

It generally takes 7-14 days to process and notify the Chief Investigator of the outcome of a request for a variation.

Major changes, depending upon the nature of your request, may require submission of a new application.

Audits:
All active ethical clearances are subject to random audit by the UHREC, which will include the review of the signed consent forms for participants, whether any modifications / variations to the project have been approved, and the data storage arrangements.

End of Document

RM Report No. E801 Version 4

Page 2 of 2

Figure A.6 Ethics certificate for survey phase 2 – page 2

Appendix B
Survey – Survey invitation eMails

Email Invitations sent to recruit participants for each phase of the survey are given below.

B.1 SURVEY INVITATION EMAIL FOR PHASE 1

Dear Student,

In July 2012 the national PCEHR (Personally Controlled Electronic Health Record) system will be available for all Australians. Both patients and healthcare professionals are expected to be familiar with this new health record system.

It is our pleasure to invite you to participate in an online survey on Electronic Health Record (eHR) system usage and acceptance. As future healthcare professionals of Australia, your participation in this survey is invaluable and greatly appreciated. The results from this survey will help develop better e-health services in the Australian healthcare sector.

This survey is part of a joint project between the Queensland University of Technology and the National ICT Australia (NICTA). The aim of the research is to design and develop an Information Accountability Framework for e-health systems.

Participation is voluntary and there will be no reimbursements, payments or otherwise (e.g. gift vouchers) for completing the survey.

This is an anonymous survey. Your participation and the answers you give cannot be traced back to you at any point during or after the survey.

Please click on the link below:

- to access further information about the study to ensure your decision and consent to participate is fully informed
- to complete the survey which will take approximately 15 minutes of your time and become part of this valuable venture

Web link to survey was here

Once again, your response helps improve the development of e-health services and to identify the requirements of the present and future consumers of e-health systems.

Thank you in advance.

Yours Sincerely,

Randike Gajanayake [1], Dr. Tony Sahama [1], Adjunct Prof. Renato Iannella [1, 2]

[1] Computer Science Discipline, Faculty of Science and Technology, Queensland University of Technology

[2] Semantic Identity, Brisbane, Australia

B.2 SURVEY INVITATION EMAIL FOR PHASE 2

Dear Students,

It is our pleasure to invite you to participate in an online survey on Electronic Health Record (eHR) system usage and acceptance. Your participation in this survey is invaluable and greatly appreciated. The results from this survey will help develop better e-health services in the Australian healthcare sector.

This survey is part of a joint project between the Queensland University of Technology and the National ICT Australia (NICTA). The aim of the research is to design and develop an Information Accountability Framework for e-health systems.

Participation is voluntary and there will be no reimbursements, payments or otherwise (e.g. gift vouchers) for completing the survey.

This is an anonymous survey. Your participation and the answers you give cannot be traced back to you at any point during or after the survey.

Please click on the link below:

- to access further information about the study to ensure your decision and consent to participate is fully informed
- to complete the survey which will take approximately 15 minutes of your time and become part of this valuable venture

Web link to survey was here

Once again, your response helps improve the development of e-health services and to identify the requirements of the present and future consumers of e-health systems.

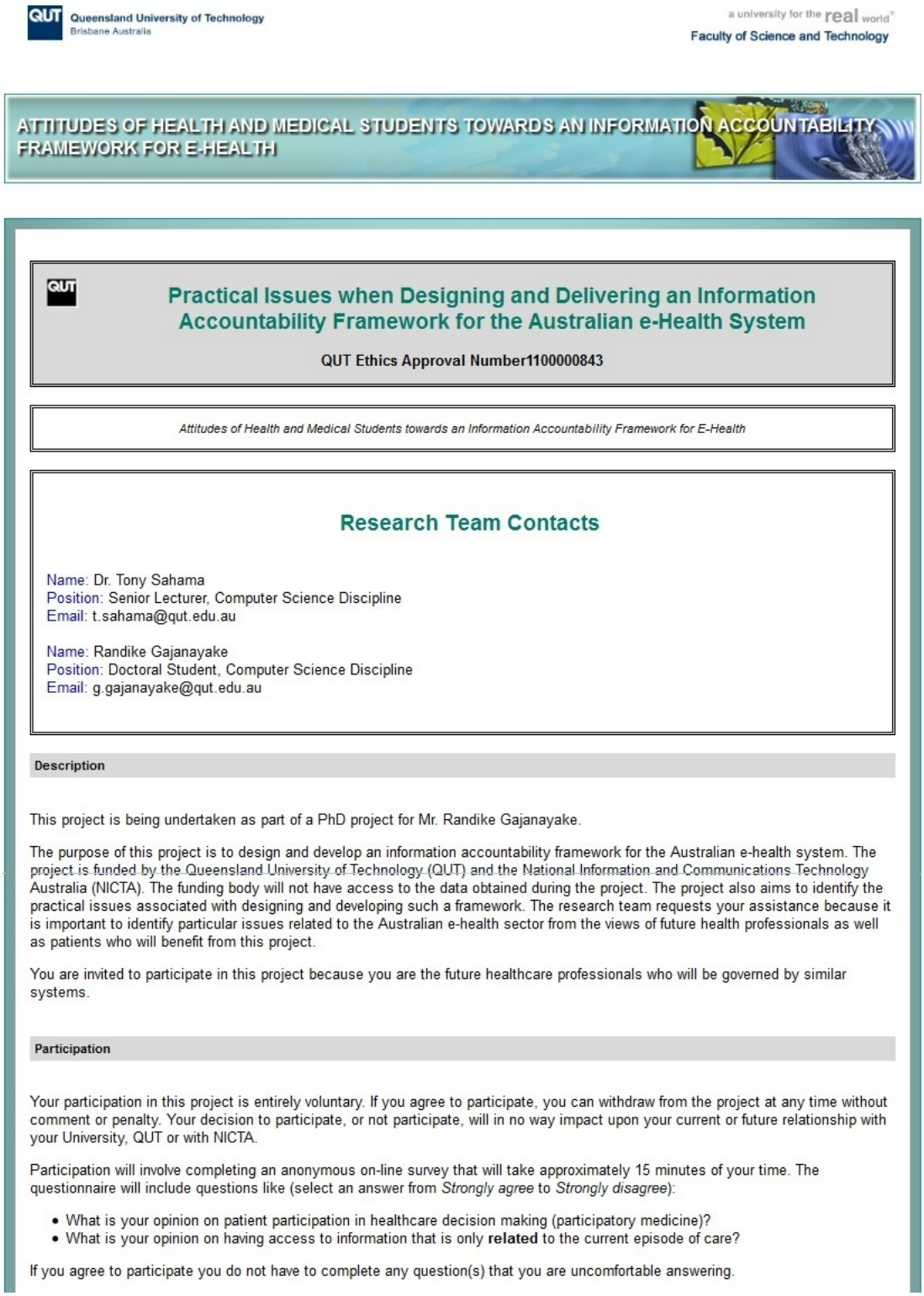
Thank you in advance.

Yours Sincerely,

Randike Gajanayake
Computer Science Discipline,
Science and Engineering Faculty,
Queensland University of Technology
Brisbane, Australia

Dr. Tony Sahama
Computer Science Discipline,
Science and Engineering Faculty,
Queensland University of Technology
Brisbane, Australia

B.3 SURVEY TOOL: PARTICIPANT CONSENT FORM FOR PHASE 1



Queensland University of Technology
Brisbane Australia

a university for the real world
Faculty of Science and Technology

ATTITUDES OF HEALTH AND MEDICAL STUDENTS TOWARDS AN INFORMATION ACCOUNTABILITY FRAMEWORK FOR E-HEALTH

Practical Issues when Designing and Delivering an Information Accountability Framework for the Australian e-Health System

QUT Ethics Approval Number1100000843

Attitudes of Health and Medical Students towards an Information Accountability Framework for E-Health

Research Team Contacts

Name: Dr. Tony Sahama
Position: Senior Lecturer, Computer Science Discipline
Email: t.sahama@qut.edu.au

Name: Randike Gajanayake
Position: Doctoral Student, Computer Science Discipline
Email: g.gajanayake@qut.edu.au

Description

This project is being undertaken as part of a PhD project for Mr. Randike Gajanayake.

The purpose of this project is to design and develop an information accountability framework for the Australian e-health system. The project is funded by the Queensland University of Technology (QUT) and the National Information and Communications Technology Australia (NICTA). The funding body will not have access to the data obtained during the project. The project also aims to identify the practical issues associated with designing and developing such a framework. The research team requests your assistance because it is important to identify particular issues related to the Australian e-health sector from the views of future health professionals as well as patients who will benefit from this project.

You are invited to participate in this project because you are the future healthcare professionals who will be governed by similar systems.

Participation

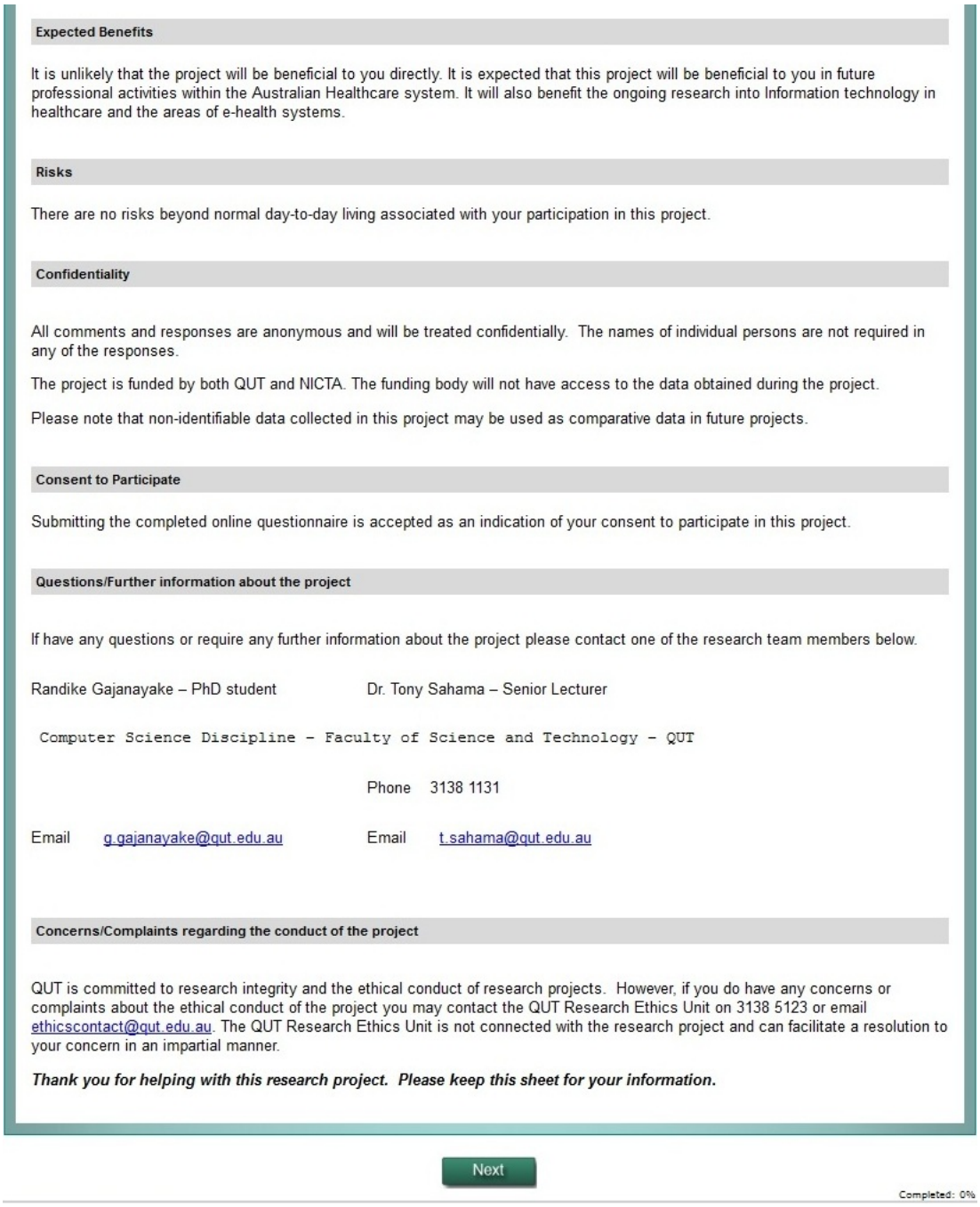
Your participation in this project is entirely voluntary. If you agree to participate, you can withdraw from the project at any time without comment or penalty. Your decision to participate, or not participate, will in no way impact upon your current or future relationship with your University, QUT or with NICTA.

Participation will involve completing an anonymous on-line survey that will take approximately 15 minutes of your time. The questionnaire will include questions like (select an answer from *Strongly agree* to *Strongly disagree*):

- What is your opinion on patient participation in healthcare decision making (participatory medicine)?
- What is your opinion on having access to information that is only **related** to the current episode of care?

If you agree to participate you do not have to complete any question(s) that you are uncomfortable answering.

Figure B.1 Survey consent form: Part 1



Expected Benefits

It is unlikely that the project will be beneficial to you directly. It is expected that this project will be beneficial to you in future professional activities within the Australian Healthcare system. It will also benefit the ongoing research into Information technology in healthcare and the areas of e-health systems.

Risks

There are no risks beyond normal day-to-day living associated with your participation in this project.

Confidentiality

All comments and responses are anonymous and will be treated confidentially. The names of individual persons are not required in any of the responses.

The project is funded by both QUT and NICTA. The funding body will not have access to the data obtained during the project.

Please note that non-identifiable data collected in this project may be used as comparative data in future projects.

Consent to Participate

Submitting the completed online questionnaire is accepted as an indication of your consent to participate in this project.

Questions/Further information about the project

If have any questions or require any further information about the project please contact one of the research team members below.

Randike Gajanayake – PhD student — Dr. Tony Sahama – Senior Lecturer

Computer Science Discipline – Faculty of Science and Technology – QUT

Phone 3138 1131

Email g.gajanayake@qut.edu.au — Email t.sahama@qut.edu.au

Concerns/Complaints regarding the conduct of the project

QUT is committed to research integrity and the ethical conduct of research projects. However, if you do have any concerns or complaints about the ethical conduct of the project you may contact the QUT Research Ethics Unit on 3138 5123 or email ethicscontact@qut.edu.au. The QUT Research Ethics Unit is not connected with the research project and can facilitate a resolution to your concern in an impartial manner.

Thank you for helping with this research project. Please keep this sheet for your information.

Next

Completed: 0%

Figure B.2 Survey consent form: Part 2

Appendix C
Survey Tool for Questionnaire

A screen capture of the online survey tool used for phase 1 is shown below.

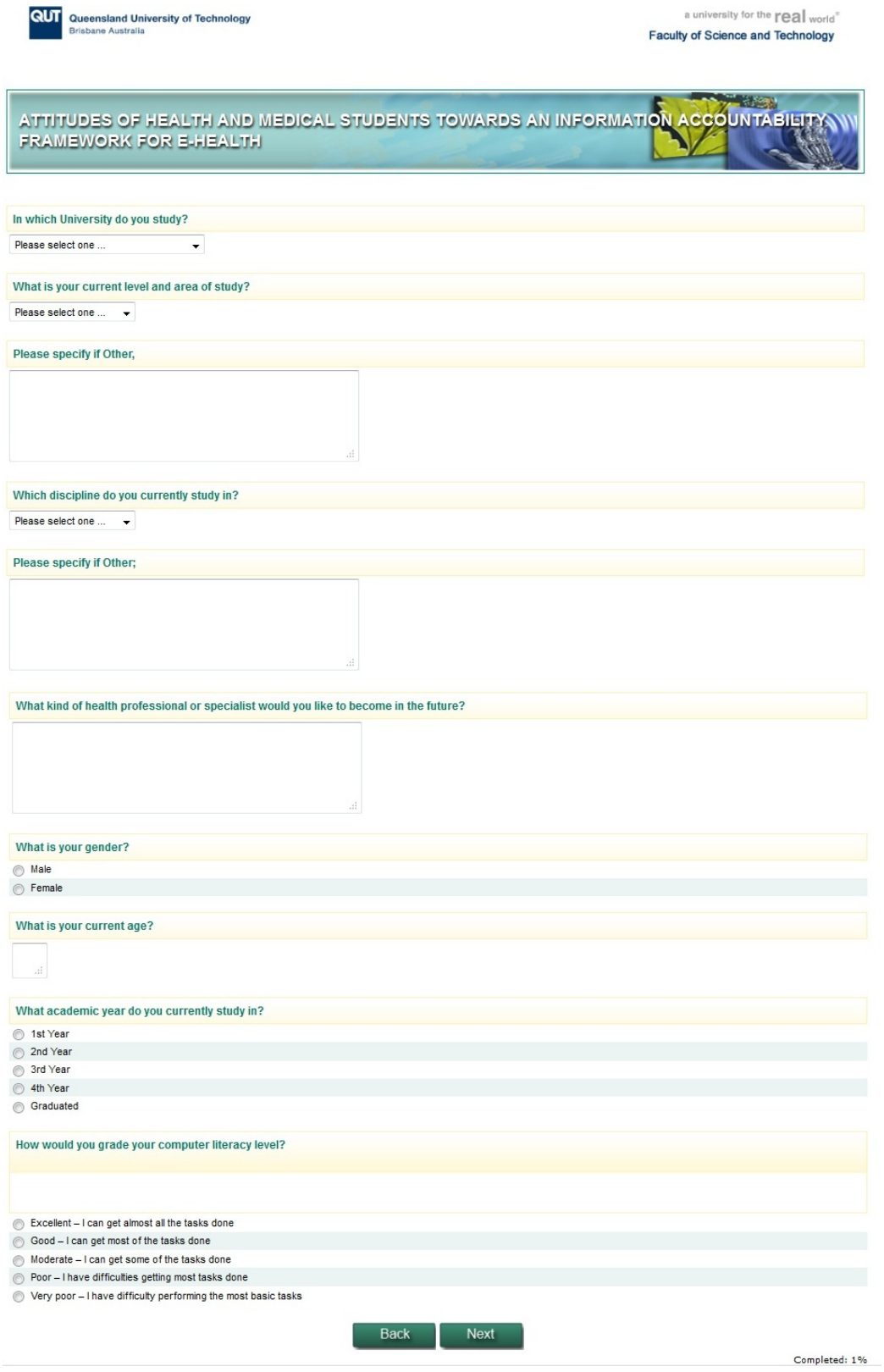


Figure B.3 Page one of the online survey tool

Appendix D
Survey Phase 1 – Qualitative data table

The comments from the survey respondents have been analysed and are summarised into categories. Table C.1 show the comments made by the respondents.

Table D.1 Data from qualitative analysis

Theme	Comments
Data Access/Availability	*I think access to patient electronic files should be the same as paper files. In a hospital setting many health care providers need access in order to provide the best possible treatment and outcome for the patient.* *Doctors often need to access patient records independently of current health care for research, auditing, checking how other similar patients have been treated, teaching other doctors and medical students etc.* *I believe information that is used for research that does not yield a personal profit should be able to be accessed to help identify causes of disease that can only otherwise be studied by intentionally placing a person in potential harm.* *I think that depending on what the patient states as to whether or not their case, without revealing who they are, can be used for further research, as an example or for medical reports in the case of anomalies.* *...I work with high risk families, sometimes accessing information on clients helps build a better picture on risk vs. protective factors. Some clients may not want us to have access to this information? What is right? Especially when dealing with children.* *If the information is used for research then there is an issue regarding informed consent. If the information is used for any reason other than patient care, or teaching within the facility/ward in which the patient is receiving care (which will influence their better care directly/indirectly) then there will have been a breach of confidentiality.* *Using an electronic health record would raise concerns about confidentiality. When placing information on the client's record, one would not be able to ensure that the information is confidential. Even if there were rules governing access, some professions may not abide by these, or may have different laws that regulate their handling of information. As a psychologist in this case I am legally responsible if someone else gains access to my client's health information without their consent - and I would not be prepared to take the risk that other health professionals would*

	respect confidentiality. Also, a great deal of client information is constructed only for a specific audience. For example, psychological reports will be written differently depending on whether they are intended for a parent, teacher, doctor or so on. As such, it would be inappropriate for other health professionals to have access to this information without having to go through the author. *I think that all health professionals should have access to the patients full medical records. Knowing the medical history for a person is important not just to know what operations or conditions they have experienced etc, they are also important to let you know how many health difficulties they have been through, which can impact on their motivation, psychology and how important they may deem your service. It is all relevant, not only for medical understanding purposes but also for understanding how interested they may in what you have to say and what stage of behaviour change they may be. I think depriving health professionals of certain information could be extremely detrimental. All health cases are different and who's to say that certain information is relevant in one case but not relevant for another. That would be extremely complex to work out and I do not think health professionals will be very happy with it at all. I know I surely wouldn't. And I would feel as if my ability to treat the patient successfully was being compromised. I also think that government bodies need people's health records (once individual information has been stripped) for research!! this is so important!! if we cannot monitor and research cases we are never going to have advances in health services and treatments, and how will we know where to focus our health campaigns?!* *The information given should only be used for the reason that it is given.* *confidentiality and respect for persons are strong values of the health industry, therefore personal information should be treated how you would like your own treated/accessed* *I think eHR is defiantly a good thing but patient information needs to be kept save and should not be access by people outside the health field like insurance companies for example* *Health information should be kept private and only patient and doctors who are treating the patient could access the patient's info...* *I believe that EHR should be freely accessible to health professionals, and that they should be able to access the patients' complete medical history….* *There are times when accessing information about episodes of care in a de-identified fashion is vital for health research that may lead to improved delivery of health care (e.g. epidemiological research)…* *It seems like a good idea but there has got to be some restrictions on the access of this information. That being said, it is sometimes necessary to look at the patients' entire history to give them the best possible care. This includes looking at things in the past that may not seem to be clearly linked to the current issue.*

	To be fair, often information not pertaining to the current episode of care is required to be accessed to collate a comprehensive past history & formulate the bigger picture. This enables health professionals across the multi disciplinary team to better assess the patient when they may be unable or unwilling to communicate vital information
Accountability Measures/ Information Misuse	*...I feel like I would like to know everything possible about the patient in order to give them the best possible care - however if patients are able to see which information I access, I would be hesitant to do so, in case it attracts litigation.* *...I agree strict usage policies should apply and heavy fines imposed on those who incorrectly use the system…* *Yes, because this information should be treated as confidential and private. No one has the right to misuse the information for other tasks other than the purpose of patient care.* *Privacy is a huge issue misuse use should be penalised strictly* *Misuse would breach patient privacy and, if done intentionally, the offender should be held accountable.* *Patient health information is confidential and it is unethical to misuse patient health information. If a health professional misuses patient health information then they should definitely be held accountable for their actions and should justify why they have misused the patient's health information. The health professional should receive appropriate punishment for this action as well.* *As in any other situation if information is misused for someone's benefit other than the patient, then it is a breach in the patient's privacy and trust also.* *...However with electronic information there can be an avenue for information misuse and I believe there should definitely be strict rules about who can access information and when.* *My father's health information and treatments were mysteriously removed from the system of the hospital where he was treated when he attempted to go to court over being negligently misdiagnosed which lead to extensive further damage to his body and longer recovery time. This information should not have been accessible, so therefore shouldn't have disappeared without knowing who had accessed them last. It should have been monitored.* *A tough and consistent rules, policies, regulations and punishment should be applied to anyone misusing patient's information, no exception at*

	all!! *I think it is unethical to misuse a patient's health information. Health Professionals need to be people we can trust and if they misuse that trust, it will hamper further treatment for the future.* *...I also think that each time a person's record is accessed it should be recorded and randomized audits of each time would ensure there is no misuse of this system…*
Patient Control	*...just don't like the idea that patients will restrict the type of information I can access. How is a patient to know if past medical history is relevant or not?* *The average patient does not know what information is relevant and what is not relevant to their health, whereas health professionals do have this knowledge. Therefore, allowing the average person to decide what medical history to show a doctor is going to have detrimental effects and could even cost someone their life.* *Duty of care to the patient. It is there information and they should use their information confidentially and use it only for the service required not for anything else that was not prior requested by the patient. The patient should have the right to refuse.* *they first need patient permission* *...In terms of privacy settings I'm not quite sure how it would work, but choosing which health professionals can or cannot see their information I think is ridiculous because the patient doesn't always have the education to realise what role different health professionals play in the treatment of their condition.* *I think that the privacy settings should not be overridden by any health care professional without patient consent. Also while university educated professionals will find this technology easy to understand, some patients may not which will affect their abilities to set appropriate privacy settings to their will.* *Patient health information is personal and private and whether electronic or paper is susceptible to miss use by health professionals. Electronic sources are easier tag for login users. Letting patients put locks on information may inhibit care by omitting important info. Information may need to be shared between professionals to confer diagnosis. if patients are able to lock out information they must also realise there is accountability to themselves if healthcare is compromised due to this.*

	it depends on if that information from a previous admission or visit is relevant to this episode, but the patient may think it is not. *...I do not think that there should be any need for patients to be able to pick and choose which information can be viewed freely or hidden as I believe it is all necessary for health professionals to be able to see it all in order to form a complete and accurate picture of the patient and to provide effective patient care.* *I think patients should have total control over their electronic record, but there could be pages for medical information and sharing amongst other health professionals.* *There should be privacy settings but i think these should be only towards other people so that strangers can't access the users information. in regards to health professionals, all of the patients/consumers details should be readily accessible to determine the best possible care.* *I am involved in hospital infection surveillance activities. This would become very difficult and place patients and health care workers at increased risk if we were denied access by patients to their information, say if a patient blocked infection control professionals access to their information. Understanding what is happening when there is an increase in infection rates will also often require an understanding of the patients involved e.g. caesarean section risk factors for surgical site infection. Additionally, for larger data linkage studies etc it becomes very difficult when patient (de-identified) information is denied. This is really less than ideal, meaning that powerful, useful studies that will ultimately benefit patient outcomes are hindered or indeed made impossible. I fully endorse patient participation but I think it needs to be well thought through, as many in the public will not understand the problems caused by blocking access in some circumstances.* *If patients are setting privacy settings so that other (non-health workers) cannot see their history that is okay, but it is essential that the treating health care professional has access to the entire medical history.* *the current rules governing pt confidentiality and information sharing should still apply. E records open up the possibility of a lot more people being able to access pt info so strict auditing will need to be applied. Pts should not be able to restrict information relevant to their treatment or what's the point of having an E record*
Attitudes on Overall System	*Overall I am for the idea, just don't like the idea that patients will restrict the type of information I can access. How is a patient to know if past medical history is relevant or not? I feel like I would like to know everything possible about the patient in order to give them the best possible care - however if patients are able to see which information I access, I would be hesitant to do so, in case it attracts litigation.* *Having seen the fallout from poor or no information sharing between professionals, trying to remedy situations without full access to the facts, and workers terrified to share information due to fear of breaching "privacy" (often with no clear understanding of what this means) I think this*

	system would be invaluable. *Patient confidentiality is an extremely important part of building the trust that allows a patient to communicate openly with you as a health professional. Misuse of private patient information, regardless of whether it is in the interest of learning or sharing knowledge breaches this trust and patients have a right to know if this is happening. If this system prevents the misuse of private patient information then I think it is worthwhile software. However the issue of hacking needs to be given consideration, as computer programs are so easily hacked and information about patients could be taken and distributed or used inappropriately.* *I think this needs further debate* *I think that the EHR is a good idea, and would benefit healthcare enormously, through the connection of different health professionals and healthcare settings. The healthcare professional would be able to have a more comprehensive view of things, and this would be beneficial for the patient, and for the health professional in making informed decisions and providing better quality healthcare. I definitely think it should be implemented within contemporary healthcare settings* *...if you were to implement this great idea you would have to hold training session and prepare work places really well. Maybe even call centres for inquires and faults.* *Depending on the level of care-this system would benefit both parties-it can be up to the discretion of the patient to add more social networks. With the main source on client care and feedback say is in the bedside chart. But this should be locked for those viewers only. They can pretty it up and add family to see progress in certain boxes-fields. However this would mean allowing time for health care workers to follow issues or concerns. This can be viewed on a tablet-such as ipad and the health worker could have all clients/patients linked to that one account. Then only are they accountable for their actions onus is not on the next worker. Obviously there would be check boxes etc procedures to follow.* *An eHR will give more timely and accurate health care to clients. Improving health outcomes, and also future collection of medical history information for research purposes. It can never replace the need for bedside observations and notes for current health episode. Overall, however, I can't believe this has not been implemented sooner*
Attitudes Towards EHR/eHealth	*eHR would significantly improve patient care flow, ensure same-time filing, ensure an accurate record of the patient consultation is recorded, allows access to previous history (should it be required i.e. surgeons) allows them to access information re: initial injury, follow-up and even to monitor post-op progress. It provides a holistic care structure where information can be safely stored. Reports and imaging can be directly uploaded on to the database and kept... ...I currently work for the ADF and I know that within this specific area, eHR would be an invaluable tool as members are constantly being posted and deployed to numerous locations around Australia and the World. It would save on "missing"*

	paperwork and delayed appointments/reviews due to constant chasing up and reprinting information/reports. I strongly believe eHR are the way of the future and should be utilised within all health facilities. *I hold currently hold qualifications in health promotion and health informatics and I'm very keen to see eHRs develop in Australia.* *The problem is one of health literacy and understanding my health professionals. The health system is extremely complex and most people have extreme difficulty navigating the system (as do the professionals). E health has the potential to improve the channels between professionals but there needs to be a change to the existing culture of destruct between professionals and the individual and between professionals.* *I believe that an electronic health care record would be very helpful in keeping patient records together and to save time from having to track down information from other professionals….* *I only don't like the idea of having patient information electronically because it would provide more opportunities for hackers and therefore more invasions of privacy/confidentiality, since once something is online "out there", it's out there, rather than having paper records which would only be immediately accessed by the hospital/facility which contains it. Also if we are fully relying on technology to access patient information needed in order to better treat them, there are always times when there are problems with technology, it either crashes or freezes, something goes wrong etc., which then makes things much more difficult.* *Electronic EHR would be a great way to save time and man power but in other ways nothing beats holding a sheet of paper hard copy of information. Does this mean every health care professional will carry around an ipad. Technology changes allllll the time and upgrades would be regular...* *A system should - be user friendly - have safeguards - involve the patient - only be used in the interest of overall patient care - should be developed with input from a range of health care professionals and organisations, not only one such as QLD health but also with input from public, private areas and orgs where this type of system is in place and highlights the positive and negatives of the system.* *...EHealth is only good for people who can/have access the internet.* *Even if health professionals are trained to use the system, not all professionals feel comfortable with using computers and therefore this could affect the quality of health care they can provide. If patients are also using the system there is the same problem. Some patients may not feel comfortable with the new technology.* *I do not trust that Queensland Health could effectively implement a eHealth record information system or guidelines for usage. IT systems and processes in Queensland Health are often outdated, overly bureaucratic, and unresponsive to needs of end users. These views are based on my personal experience with implementation of a clinical electronic system in Queensland Health. The recent payroll issues would also highlight*

	lack of expertise, planning, problem solving in implementation of electronic solutions in Queensland Health and other Queensland Government entities. I believe an electronic health record can work effectively to improve documentation and communication but would require huge expenditure and vastly improved systems for implementation to be effective. *I think an effective eHealth network needs to be extremely user friendly with an easy to navigate user interface. I think assurances need to be given about the quality of information storage and back-up retrieval systems if the eHealth network falls short i.e. during software patch updates. I don't think QLD Health could organise a meat-tray raffle let alone "formulate a comprehensive set of usage rules which would indicate what health data is required for a given episode of care". Having this Utopian vision of a universal eHealth network is already flawed because there are so many versions of some form of e-documentation operating in so many hospitals.* *Can't wait for the eHealth record so it will reduce time and potential errors brought about by misinterpretation of handwritten orders/assessment* *Having worked on an eHealth system with QH* (Queensland Health) *I can recognise the limitations of a computer system. It can often be incapable of performing a task required by clinicians in a simple way that is not cumbersome.* *Still being a student it is hard for me to comment on a lot of these things because I have not been out in the hospital work place and experienced it. I think that having electronic files would make things easier in the sense that paper things can go missing, its difficult to read peoples handwriting sometimes, and if its online anyone can access it regardless of where they are in the hospital (i.e. don't have to walk up into a certain level to get the paper records or anything) and it would be easy to then forward these records electronically onto someone's GP/specialist/outpatient setting. It would also save space if everything is online and not on paper.*
Other	*First of all I think a comment section should have been included after every question as I wanted to make comments on a lot of them. My main concern given my interest is in mental health that inappropriate labelling could be entered and follow a patient for life, e.g. one 'professional' may label a patient non-compliant because they didn't want to be put on drug therapy against their wishes and this would follow a patient regardless of the fact that the force of drugs is against basic human rights... but then that is something not totally acknowledged by the mental health system. As for who monitors the system I think it needs to be a totally independent and accountable body and not the new 'mental health commission' as that is not independent it is just a change of name.*
Note: 1. Some comments have been adjusted to eliminate spelling and grammatical errors.	

Appendix E
Survey Phase 2 – Tables

The data table relevant to chapter four are given in the Appendix.

Table E.1 Qualitative data from respondents

Theme	Comments
Information misuse and Accountability measures	*Sometimes may need more than civil ($$) penalties, but there are many grey areas in health IT. It is difficult to know what may happen without Australian court precedents.* *Jail time and fines should be given* *Other than times of emergency, even health professionals should have to provide sufficient reasoning as to why a patients information has been accessed. Without sufficient safeguards sensitive health information would be accessible to anyone. The term 'Sufficient reasoning' should be up to the end user, through privacy settings NOT Government Legislators.* *If they are misused in some insidious plot to cause harm or I dunno spread my info across the Internet yeah sure. But if their intent is too better treat a patient or use the data in some reasonable medical way(such as research), only they happen to break some small rule in information usage, meant only to ensure a patients impression of privacy while limiting practical use of data, then no, they shouldnt be punished, instead the rules should be adapted to the needs of the health professionals.* *If they are found to have misused the information then that should be the same as breaking patient confidentiality. If they have used it for researching patients with conditions similar to one of their own, or to help the patientm then I do not think it is a bad thing.* *Misuse should be made a criminal offence to discourge it.* *This information is no different from a person's criminal record and police are held accountable if the access it without justifiable reason.* *Systems designed to manage health information more effectively should NOT be taken advantage of for other uses than originally intended.* *Would need to be reviewed against their intents and the potential harm to the patient.* *Of with their heads. Or a fine, either or.* *Any miss-use of private data regardless of where or how it was accessed, is still a breach of personal privacy and should be prosecutable under the full extent of the law regardless of who or what accessed the data…*

	Like everybody else, if you misuse data you should pay the penalty *I believe a monetary fine would be most effective* *The penalty would depend on the misuse. If my information is being used to sell to drug companies, without my permission for monetary gain. Then this should be a jail sentence…* *I believe that if a health professional used my personal health information for any other reason than for reference, clinical research or diagnosis then the person(s) responsible should be held accountable if they cannot legitimately justify their actions.* *If it is found to be used for something other than for medical reasons they should be accountable* *If they are doing wrong things intentionally and not in their "Duty of Care", then they must be held accountable* *If misuse is intentional then the health professional is violating the 'Good Medical Practice: Code of Conduct' guidelines for Privacy and Confidentiality. This is a breach of ethics regardless of the medium used to access the patient health information.*
Personal information in EHR	*…I see the value in other health care professionals having an anonymous set of records to help treat other patients. I was about to type in 100 years I still wouldn't want my name published with my health record. But then I realised that is selfish as my descendants might benefit from it…* *…I believe the system should log the id and name of any enquiry into my health record. I should have access to that information…* *Because it is personal, so it's important to keep it security. i agree that should take seriously.* *in conclusion, all people should manage their own health, if they can't its their responsibility to find their own health professional…*
Notification	*Misuse of health information should be reported to the health professionals registration authority.* *The electronic record should be able to be used in a court proceeding if the misuse amounts to a criminal act.*
Unauthorised access	*There is never a circumstance when misuse can be excused. But that is not the same as unauthorised access for example. which may be required under life threatening circumstances* *It should be treated as fraud/breach if privacy…*
Privacy concerns	*Really depends on the seriousness of the misuse. I haven't really thought too much about how health information could be misused, but I tend to worry less about privacy in this regard than most people. Probably a fine for a minor misuse and potential loss of job for serious misuse.* *Misusing health information is an extreme breach of trust, akin to current patient privacy expectations.* *Electronic health record should remain secure and can be opened or viewed through a series of bio metric scanning or any other possible keys.* *I would never use an eHR system if it required JavaScript or proprietary software. I would not trust a centralised government database for*

	health records; that would be like 1984.
Access to information	*…A doctor/nurse treating a patient should have full access to the complete medical history of a patient.* *Health professionals are/should be obligated to follow a set of morals and ethics or a code of conduct to be able to become and stay a health professional.* *No way is any health professional sharing my health information with any other patient!!!* *While I believe to many privacy or security restrictions on health data would limit the effective use of the information by medical professionals, I believe misuse of such information privileges should not go unpunished.* *…If someone accesses my personal data without my conscious consent (fine-print doesn't count) then that should be classed as a prosecutable breach of privacy. That being said I have some faith in my fellow IT professionals and as such would have only slight hesitation using such a eHR system…* *…It would be good if I can see who has accessed my information including for research and the type of research.* *…I trust an authority to handle my health information, If proper security and restrictions on the eHR system is made, no one else would access…*

Table E.2 Individual Item loadings

Construct	Indicators	Loading
Computer/EHR self-efficacy (CSE)	CSE1	0.9112
	CSE2	0.6983
	CSE3	0.4604
Computer/EHR anxiety (ANX)	ANX1	0.7338
	ANX2	0.8562
	ANX3	0.8848
	ANX4	0.8689
Computer/EHR attitude (ATT)	ATT1	0.7885
	ATT2	0.7924
	ATT3	0.7698
Privacy Concerns (PC)	PC1	0.9339
	PC2	0.6099
	PC3	0.7833
	PC4	0.8988
	PC5	0.7789
Third party trust (TRT)	TPT1	0.9062
	TPT2	0.7259
	TPT3	0.6882
EHR Access (ACS)	EA1	0.8357
	EA2	0.9043
EHR Sharing (SRE)	ES1	0.4536
	ES2	0.8488
	ES3	0.8740
Information governance (IG)	IG1	0.7524
	IG2	0.7683
	IG3	0.6373
	IG4	0.4958
Information control (IC)	IC1	0.8482
	IC2	0.8660
	IC3	0.8546
Information accountability (IA)	IA1	0.6906
	IA2	0.6320
	IA3	0.7379
	IA4	0.8263
	IA5	0.8000
Perceived acceptance (ACC)	ACC1	0.8526
	ACC2	0.7483
	ACC3	0.8476

Table E.3 Internal composite reliability and average variance extracted

Construct	AVE	Composite Reliability
Computer/EHR self-efficacy (CSE)	0.5100	0.7445
Computer/EHR anxiety (ANX)	0.7023	0.9038
Computer/EHR attitude (ATT)	0.6141	0.8268
Privacy concerns (PC)	0.6221	0.7592
Third party trust (TPT)	0.6073	0.8205
EHR access (EA)	0.7581	0.8622
EHR sharing (ES)	0.5634	0.7834
Information governance (IG)	0.5210	0.7627
Information control (IC)	0.7347	0.8471
Information accountability (IA)	0.5487	0.8576
Perceived acceptance (ACC)	0.7227	0.8390

Table E.4 Correlation of constructs and square root of AVE

	CSE	ANX	ATT	PC	TPT	EA	ES	IG	IC	IA	ACC
CSE	**0.714**										
ANX	-0.289	**0.838**									
ATT	0.310	-0.504	**0.783**								
PC	-0.08	0.440	-0.601	**0.788**							
TPT	0.190	-0.068	0.274	-0.300	**0.779**						
EA	-0.01	-0.05	0.189	-0.302	0.336	**0.870**					
ES	0.347	-0.284	0.459	-0.374	0.309	0.103	**0.750**				
IG	0.201	0.054	0.055	0.281	0.135	-0.220	-0.006	**0.721**			
IC	0.192	0.083	0.010	0.247	-0.286	-0.327	-0.057	0.218	**0.857**		
IA	0.245	-0.092	0.112	0.220	-0.057	-0.306	0.095	0.506	0.470	**0.740**	
ACC	0.414	-0.631	0.734	-0.508	0.236	0.107	0.516	0.074	0.042	0.120	**0.850**

Table E.5 Cross loadings of constructs

	CSE	ANX	ATT	PC	TPT	IG	IC	IA	ACC
CSE1	**0.911**	-0.350	0.328	-0.13	0.107	0.142	0.209	0.220	0.428
CSE2	**0.698**	-0.130	0.175	0.021	0.153	0.163	0.088	0.203	0.228
CSE3	**0.460**	0.044	0.058	0.001	0.288	0.199	0.053	0.062	0.123
ANX1	-0.17	**0.733**	-0.356	0.297	-0.052	0.081	0.129	0.002	-0.451
ANX2	-0.26	**0.856**	-0.402	0.327	0.005	0.036	0.011	-0.094	-0.479
ANX3	-0.26	**0.884**	-0.444	0.35	-0.043	-0.03	0.061	-0.130	-0.578
ANX4	-0.27	**0.868**	-0.473	0.475	-0.121	0.091	0.080	-0.074	-0.587
ATT1	0.200	-0.444	**0.788**	-0.47	0.103	0.035	-0.03	0.053	0.537
ATT2	0.320	-0.289	**0.792**	-0.46	0.35	0.125	0.143	0.174	0.664
ATT3	0.199	-0.466	**0.769**	-0.50	0.165	-0.04	-0.10	0.025	0.514
PC1	-0.07	0.439	-0.637	**0.933**	-0.280	0.234	0.213	0.180	-0.531

PC2	-0.07	0.206	-0.198	**0.609**	-0.181	0.235	0.191	0.190	-0.185
PC3	-0.12	-0.082	-0.088	**0.835**	-0.192	0.275	-0.30	-0.277	0.049
PC4	0.071	-0.024	-0.226	**0.848**	-0.372	0.138	-0.27	-0.260	0.127
PC5	0.125	-0.063	-0.075	**0.874**	-0.280	0.169	-0.12	-0.089	0.104
TPT1	0.099	-0.114	0.251	-0.35	**0.906**	0.016	-0.32	-0.145	0.224
TPT2	0.042	0.038	0.142	-0.13	**0.725**	0.102	-0.25	-0.086	0.067
TPT3	0.332	-0.040	0.234	-0.16	**0.688**	0.258	-0.07	0.149	0.236
IG1	0.153	-0.052	-0.024	0.272	-0.015	**0.752**	0.211	0.517	0.045
IG2	0.126	0.112	0.095	0.133	0.332	**0.768**	0.033	0.210	0.064
IG3	0.174	0.034	0.029	0.232	-0.096	**0.637**	0.245	0.367	0.021
IG4	0.121	0.017	0.022	0.187	-0.140	**0.495**	0.285	0.456	0.079
IC1	0.199	0.034	0.079	0.205	-0.193	0.194	**0.848**	0.384	0.091
IC2	0.132	0.106	-0.057	0.219	-0.294	0.180	**0.866**	0.420	-0.015
IC3	0.123	0.111	0.027	0.129	-0.154	0.109	**0.876**	0.340	-0.032
IA1	0.205	-0.133	0.149	0.127	0.051	0.498	0.330	**0.690**	0.108
IA2	0.222	-0.132	0.154	0.058	-0.071	0.407	0.317	**0.632**	0.185
IA3	0.141	-0.050	0.047	0.146	-0.180	0.197	0.423	**0.737**	0.066
IA4	0.112	0.002	-0.009	0.249	-0.031	0.332	0.323	**0.826**	0.013
IA5	0.246	-0.068	0.114	0.189	-0.005	0.455	0.369	**0.8**	0.1116
ACC1	0.450	-0.388	0.696	-0.39	0.248	0.071	0.167	0.180	**0.852**
ACC2	0.374	-0.488	-0.576	-0.245	0.210	0.067	0.129	0.102	**0.865**
ACC3	0.252	-0.687	0.551	-0.47	0.152	0.054	-0.09	0.022	**0.847**

Table E.6 Path coefficients of moderating variable Gender

	Gender		
	Male	***Female***	
PC - R^2	0.3638	0.3983	
IG - R2	0.2456	0.1357	
IC - R2	0.394	0.2693	
IA - R2	0.1735	0.0265	
ACC - R2	0.6773	0.7814	
Path coefficients with significance			**Hypothesis**
CSE -> IC	0.1656	0.3279	H1
CSE -> ACC	0.1466	-0.0092	H2
ANX -> PC	0.1799**	0.1461	H3
ANX -> ACC	-0.2748**	-0.1413	H4
ANX -> IC	0.149	-0.011	H5
ATT -> PC	-0.3546***	-0.3874**	H6
ATT -> ACC	0.5548***	0.7013***	H7
ATT -> IC	0.362**	0.097	H8
PC -> IG	0.5403***	0.3621	H9
PC -> IC	0.464***	0.2652*	H10
PC -> IA	0.4312***	0.1103	H11

PC -> ACC	-0.1078	-0.0574	H12
TPT -> PC	-0.2942***	-0.3119	H13
TPT -> IG	0.2067	-0.0148	H14
TPT -> IC	-0.2763**	-0.2829	H15
TPT -> IA	0.0411	-0.0829	H16
TPT -> ACC	0.0581	0.2079	H17
IG -> ACC	0.0784	-0.0413	H18
IC -> ACC	0.0647	0.1188	H19
IA -> ACC	-0.0788	-0.02	H20

Table E.7 Path coefficients of moderating variable Age

	Age			
	17-21	***22-31***	***32-65***	
PC - R^2	0.5304	0.2812	0.3856	
IG - R2	0.2141	0.3167	0.2988	
IC - R2	0.4427	0.2941	0.3567	
IA - R2	0.1173	0.1841	0.1126	
ACC - R2	0.7215	0.7566	0.7691	
Path coefficients with significance				**Hypothesis**
CSE -> IC	0.2459**	0.2335	0.3007	H1
CSE -> ACC	0.118	0.0782	0.0592	H2
ANX -> PC	0.3425**	0.1899	-0.0842	H3
ANX -> ACC	-0.147	-0.4328***	-0.1193	H4
ANX -> IC	-0.051	0.192	0.153	H5
ATT -> PC	-0.3635**	-0.2919	-0.5133	H6
ATT -> ACC	0.6453***	0.4203***	0.6375***	H7
ATT -> IC	0.332*	0.263	0.388	H8
PC -> IG	0.507**	0.5883***	0.461*	H9
PC -> IC	0.5651***	0.3498**	0.3965	H10
PC -> IA	0.3761	0.4378***	0.3724	H11
PC -> ACC	-0.0578	-0.1687	-0.1258	H12
TPT -> PC	-0.2667	-0.27*	-0.1739	H13
TPT -> IG	0.2433	0.2943	-0.1405	H14
TPT -> IC	-0.1839	-0.3345***	-0.1517	H15
TPT -> IA	0.1629	0.0287	0.2936	H16
TPT -> ACC	0.1124	0.141	-0.0404	H17
IG -> ACC	0.1632	0.0152	-0.2035	H18
IC -> ACC	0.1153	0.123	0.084	H19
IA -> ACC	-0.1447	-0.0345	0.1891	H20

Table E.8 Path coefficients of moderation variable Computer Literacy

	Literacy	
	Excellent	***Good***
PC - R^2	0.3479	0.5267
IG - R2	0.2317	0.1937
IC - R2	0.3438	0.3019
IA - R2	0.0957	0.1884
ACC - R2	0.6931	0.6794
Path coefficients with significance		**Hypothesis**
CSE -> IC	0.2663**	0.1313	H1
CSE -> ACC	0.1453	0.1292	H2
ANX -> PC	0.1398*	0.1925	H3
ANX -> ACC	-0.321***	-0.5553	H4
ANX -> IC	0.042	0.148	H5
ATT -> PC	-0.4228**	-0.3984	H6
ATT -> ACC	0.467***	-0.062*	H7
ATT -> IC	0.269**	0.435	H8
PC -> IG	0.3989***	0.1775	H9
PC -> IC	0.2558***	0.0355	H10
PC -> IA	0.2155**	0.0864	H11
PC -> ACC	-0.0644	-0.1759	H12
TPT -> PC	-0.208***	0.312	H13
TPT -> IG	0.2427	0.3011	H14
TPT -> IC	-0.261***	0.2401	H15
TPT -> IA	-0.031	0.5222	H16
TPT -> ACC	0.0082	-0.0885	H17
IG -> ACC	0.0873	0.2543	H18
IC -> ACC	0.0602	-0.2856	H19
IA -> ACC	-0.0227	-0.1749	H20

Table E.9 Path coefficients of moderating variable PCEHR awareness

	PCEHR	
	Aware	***Not Aware***
PC - R^2	0.4003	0.3753
IG - R2	0.223	0.4004
IC - R2	0.3903	0.2098
IA - R2	0.1269	0.0939
ACC - R2	0.7053	0.8001
Path coefficients with significance		**Hypothesis**
CSE -> IC	0.2089**	0.156	H1
CSE -> ACC	0.1908**	-0.1206	H2
ANX -> PC	0.1955**	0.1161	H3

ANX -> ACC	-0.338***	-0.3578	H4
ANX -> IC	0.036	0.056	H5
ATT -> PC	-0.4485**	-0.5678	H6
ATT -> ACC	0.483***	0.466	H7
ATT -> IC	0.346**	0.166	H8
PC -> IG	0.2313**	0.4532	H9
PC -> IC	0.1745***	0.302	H10
PC -> IA	0.2628**	0.0028	H11
PC -> ACC	-0.0031	-0.0357	H12
TPT -> PC	-0.229***	-0.0594	H13
TPT -> IG	-0.258	0.4085	H14
TPT -> IC	-0.339**	0.0069	H15
TPT -> IA	-0.1387	0.2603	H16
TPT -> ACC	0.045	0.3648	H17
IG -> ACC	0.0611	-0.0606	H18
IC -> ACC	0.0785	0.0892	H19
IA -> ACC	-0.155**	0.1722	H20

Appendix F
UPPAAL Automata

The UPPAAL automata for the modelling of the technical architecture in chapter seven are shown below.

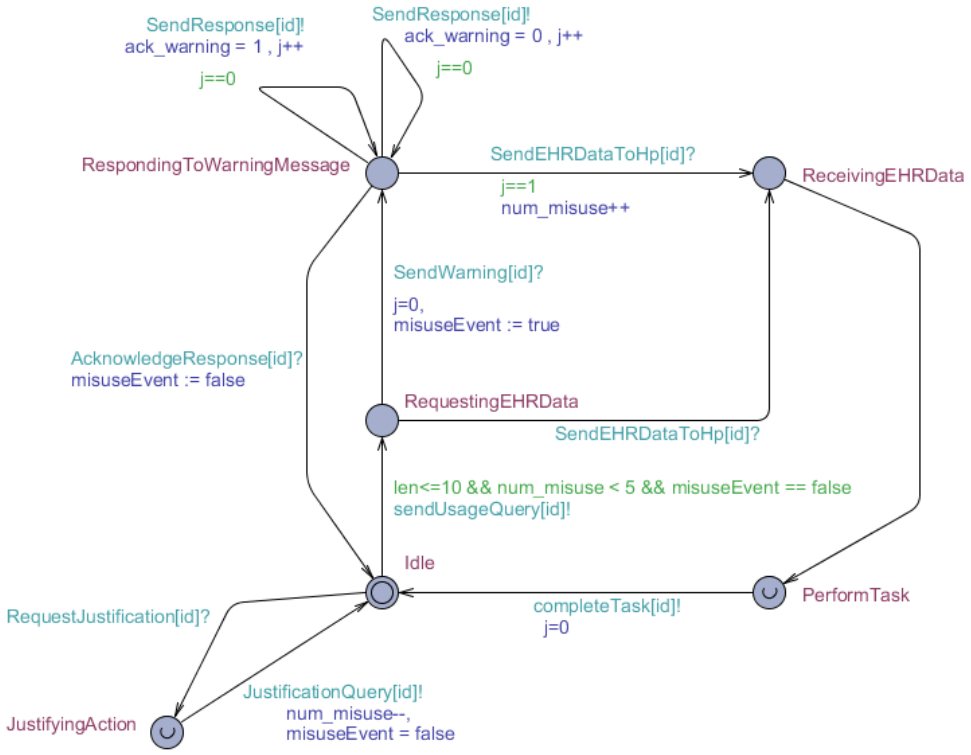


Figure F.1 Healthcare professional service UPPAAL model

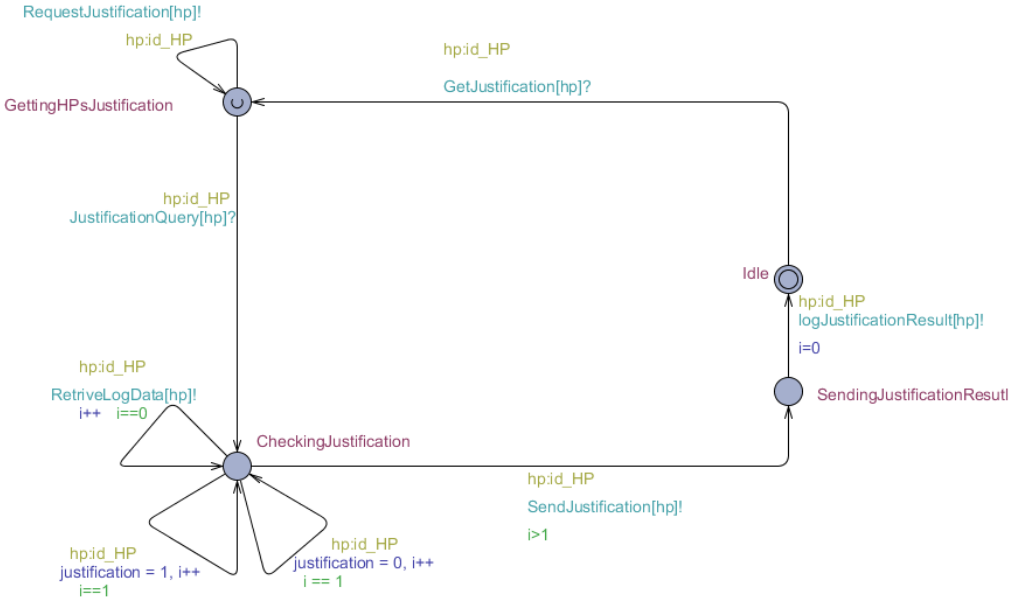


Figure F.2 Policy reasoning service UPPAAL model

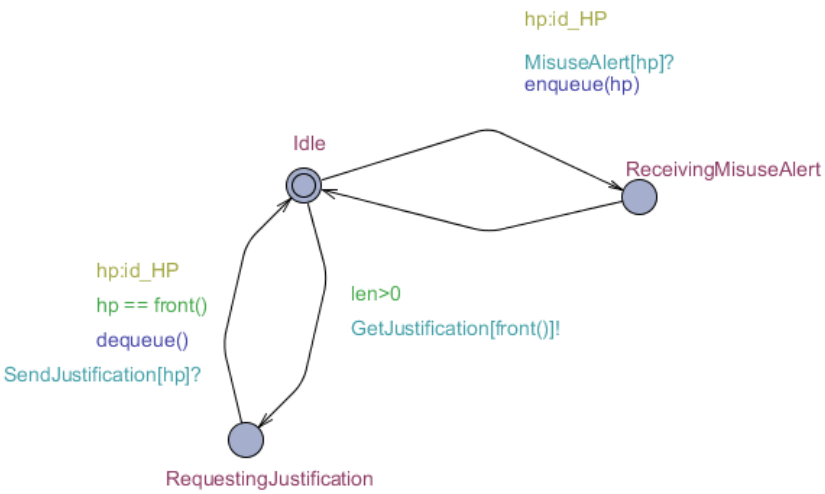


Figure F.3 Patient Service model in UPPAAL

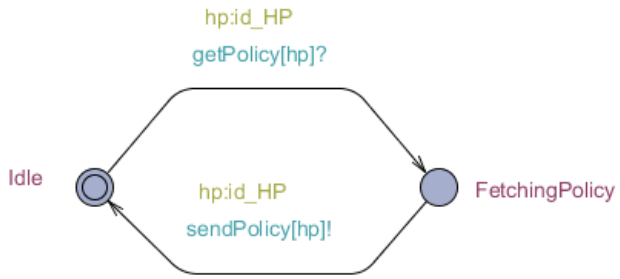


Figure F.4 Policy Service model in UPPAAL

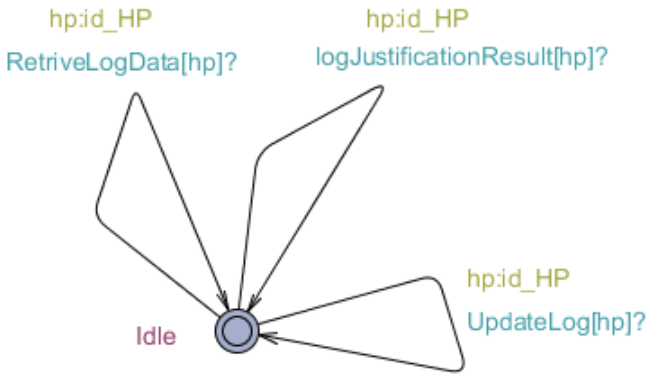


Figure F.5 Transaction Logging Service in UPPAAL

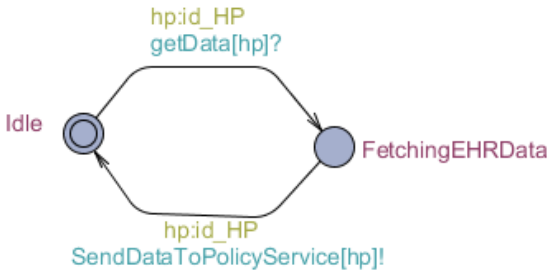


Figure F.6 Data Service in UPPAAL

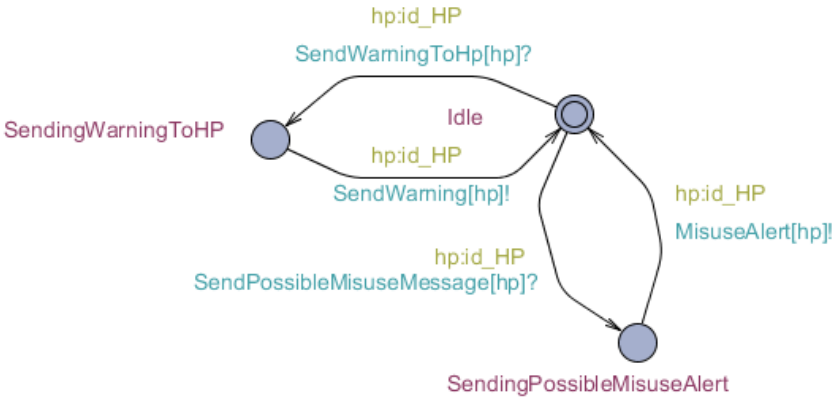


Figure F.7 Message Service in UPPAAL